

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
7 October 2004 (07.10.2004)

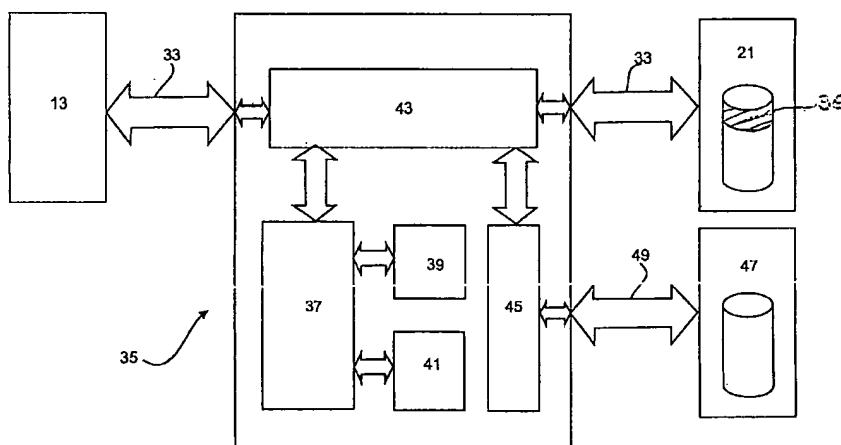
PCT

(10) International Publication Number
WO 2004/086228 A1

- (51) International Patent Classification⁷: G06F 12/14, 1/00 (74) Agent: WRAY & ASSOCIATES; Level 4, The Quadrant, 1 William Street, Perth, Western Australia 6000 (AU).
- (21) International Application Number: PCT/AU2004/000387 (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (22) International Filing Date: 29 March 2004 (29.03.2004)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 2003901454 28 March 2003 (28.03.2003) AU
- (71) Applicant (for all designated States except US): SECURE SYSTEMS LIMITED [AU/AU]; Level 1, 80 Hasler Road, Osborne Park, Western Australia 6017 (AU).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): KABZINSKI, Richard [AU/AU]; 5 Balladonia Drive, Ellenbrook, Western Australia 6069 (AU). HEARN, Michael, Alfred [AU/AU]; 1 Urawa Road, Duncraig, Western Australia 6023 (AU). POWERS, Russell, E. [AU/AU]; Level 1, 80 Hasler Road, Osborne Park, Western Australia 6017 (AU).
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- Published:
— with international search report

[Continued on next page]

(54) Title: SECURITY SYSTEM AND METHOD FOR COMPUTER OPERATING SYSTEMS



(57) Abstract: A security system for a computer operating system comprising a processor (37) that is independent of the host CPU (13) for controlling access between the host CPU (13) and a security partition formed in the storage device (21) for storing the operating system. A program memory (41) that is independent of the computer memory and the storage device (21) unalterably stores and provides computer programs for operating the processor (37) in a manner so as to control access to the security partition in the storage device (21). All data access by the host CPU (13) to the data storage device (21) is blocked before initialisation of the security system and is intercepted immediately after the initialisation under the control of the processor (37). The processor (37) effects independent control of the host CPU (13) and configuration of the computer (11) to prevent unauthorised access to the security partition on the storage device (21) during the interception phase. All users of the computer (11) are authenticated with a prescribed profile of access to the operating system files in the security partition on the storage device (21) and data access to the storage device remains blocked until a user of the computer (11) is correctly authenticated.

WO 2004/086228 A1



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

- 1 -

"Security System and Method for Computer Operating Systems"**Field of the Invention**

This invention relates to a security system for securing data and information
5 stores in computer systems and a method of securing the same. More
particularly, the invention relates to a security system and method for securing an
operating system of a computer.

In the context of this specification, a computer system is defined to include a
computer having a central processing unit (CPU) and a storage device, which
10 may be a hard disk, CD R/W or other read/writeable data storage media or any
combination of the same, and a network incorporating one or more such
computers, as in a client server system.

As used herein, an operating system of a computer comprises software and data
which provide an interface between a user and the hardware of the computer, and
15 which control all other programs to be run on the computer. An operating system
may therefore handle interface to peripheral hardware, schedule tasks, allocate
storage, and present a default interface to the user when no application program
is running. The user interface may comprise a command language, graphical
user interface or window system. An operating system loader, BIOS, or other
20 firmware required at boot time or when installing an operating system are not
generally considered part of an operating system.

The term "partition" is used herein to mean a section, zone or contiguous grouping
of data blocks in a read/writeable storage device created by formatting the storage
device.

25 Throughout the specification, unless the context requires otherwise, the word
"comprise" or variations such as "comprises" or "comprising", will be understood to

- 2 -

imply the inclusion of a stated integer or group of integers but not the exclusion of any other integer or group of integers.

Background Art

- In these days of widespread computer usage, data stored on a computer system is becoming increasingly accessible to a variety of users. This may occur directly in real time via local and/or remote use of a computer system by different users or indirectly via the loading and running of computer programs at predetermined times automatically or manually by a user of the computer system. With the advent of computer networks allowing remote access to computer systems via local area networks and wide area networks such as the Internet, and the ready transfer of computer programs and data between computer systems, either manually via floppy disks and CD ROMs or automatically via computer networks, the security and integrity of data and information stored on the read/write stores of computers is becoming increasingly of paramount importance.
- 15 It is now common place for computer systems to incorporate "anti-virus" software in order to protect the data and information stored on the storage device thereof from hostile computer programs, and user authentication procedures allowing predetermined levels of access to data and information stored on the storage device of the computer system, dependent upon the status of the user.
- 20 A problem with most types of anti-virus software and user authentication protocols used today is the very fact that they are embodied in software, which is required to be executed under the control of the operating system of the computer. Hence, a pre-requisite for such anti-virus or user authentication software to function correctly is that the computer system must be able to power-on, boot-up and
- 25 invoke the operating system "cleanly", without any virus or security defeating processes affecting the computer during this time.

In the case of anti-virus software, most of this software depends upon having some knowledge of the virus or type of virus that it is attempting to secure the system from. Hence, the anti-virus software needs to be constantly updated and

- 3 -

entered onto the computer system before a particular virus finds its way to the computer system.

As certain viruses can be extremely hostile and destructive to computer systems, the lag time between the first occurrence of a virus and the production of software to combat the virus still creates a window within which oftentimes irreparable damage can occur to certain computer systems infected with such a virus. Indeed, the production of viruses and anti-virus software does have a tendency to be self-perpetuating. Thus whilst better solutions may have been proposed in the past to combat viruses and ensuring the security of data and information, the state of the art has remained around adopting a software approach to deal with the problem.

Notwithstanding this, various hardware-based solutions, which are intrinsically more reliable and resilient in preventing virus or unauthorised access to data stored on a computer system, have been proposed in the past. However, these have been awkward to apply, restricted in their adaptability to different and changing formatting standards or have required user interaction of a technical nature well beyond the mere loading of executable programs, in order to make them effective or even operational.

The operating system of a computer is typically stored on a read/writeable storage device or a CD-ROM. The abovementioned security problems apply where the operating system is stored on a read/writeable storage device such as a hard disk drive (HDD). In contrast, storing the operating system on a CD ROM provides security but sacrifices flexibility because the operating system cannot be modified, and the computer can only be operated with the CD ROM itself. Further, the operating system can only be upgraded by replacing the CD ROM.

It would be advantageous to secure an operating system for a computer in a read/writeable storage device.

- 4 -

Disclosure of the Invention

In accordance with one aspect of the present invention, there is provided a security system for an operating system of a computer having a host central processing unit (CPU), memory used by the host CPU to load programs in order
5 to operate the computer and a read/writeable storage device for storing data to be handled by the computer, the security system comprising:

a security partition formed in the storage device, wherein the operating system is stored in the security partition;

10 profiling means to define at least two different data access profiles with respect to the storage device for users of the computer, one access profile ascribing read/write access to data stored on said security partition, and the other access profile ascribing a blocking level of access that does not permit write access to said security partition; and

15 blocking means for selectively blocking data access between the host CPU and the security partition in accordance with the particular data access profile defined for a user effecting data access to the storage device at any particular point in time;

20 wherein said blocking means is independent and separately configurable of said host CPU to impose and continuously maintain the requisite level of data access to said security partition for users effecting said data access in accordance with the particular data access profile thereof regardless of the subsequent operations of the host CPU.

Preferably, the security system includes authentication means to authenticate a user of the computer having a prescribed data access profile and configure said
25 blocking means to control subsequent access to the security partition in accordance with the data access profile of that user, before that user is able to access said security partition regardless of the particular data access profile of that user.

- 5 -

Preferably, the security system includes processing means independent of the host CPU for controlling the operation of said blocking means for blocking access between the host CPU and the storage device in response to said authentication means.

- 5 Preferably, the blocking means blocks all data access by the host CPU to the data storage device before initialisation of the security system and includes intercepting means to intercept all said data access immediately after said initialisation under the control of said processing means.

- Preferably, said processing means effects independent control of the host CPU
10 and configuration of the computer in a manner so as to prevent unauthorised access to the storage device, upon said intercepting means intercepting said data access immediately after said initialisation and before loading of the operating system of the computer.

- Preferably, said authentication means enables a software boot of the computer to
15 be effected after correct authentication of the user, and said processing means permits normal loading of the operating system during the start up sequence of the computer following said software boot.

- Preferably, the security system includes program memory means independent of the memory of the computer and the storage device to unalterably store and
20 provide computer programs for operating the processing means in a prescribed manner to control said access.

- Preferably, the security system includes memory store means independent of the memory means and the storage device of the computer to store critical data and control elements associated with the basic operation of the computer and access
25 to the storage device.

Preferably, said critical data and control elements are supplied to and used by the host CPU for verification of the storage device and operating the computer independently of the storage device during the start up sequence of the computer.

- 6 -

Preferably, the authentication means includes a login verifying means to enable a user of the computer to enter a login identification and password and have that login identification and password verified to authenticate said user being an authorised user of the computer having a prescribed profile of access to the storage device before allowing the start up sequence of the computer to proceed further.

Preferably, said login identification and passwords of authorised users and the prescribed profile of access thereof form part of said critical data and control elements and said login verifying means accesses said critical data and control elements to effect authentication of a user.

Preferably, the prescribed profile of access comprises a prescribed allocation of predetermined levels of access permitted for an authorised user of the computer to prescribed partitions of the storage device. Preferably, the prescribed partitions include the security partition.

Preferably, the independent processing means and independent program memory means are adapted to be connected only in line with the data access channel between the host CPU and the storage device, and off the main data and control bus of the host CPU.

In accordance with another aspect of the present invention, there is provided a method for securing and protecting an operating system of a computer from unauthorised access, the computer having a host central processing unit (CPU), a read/writeable storage device for storing data to be handled by the computer, and memory used by the host CPU to load programs in order to operate the computer and storage device, the method comprising:-

forming a security partition in the storage device, and storing the operating system in the security partition;

defining at least two different data access profiles with respect to the storage device for users of the computer, one access profile ascribing

- 7 -

read/write access to data stored on said security partition, and the other access profile ascribing a blocking level of access that does not permit write access to said security partition;

5 selectively blocking all data access between the host CPU and the security partition in accordance with the particular data access profile defined for a user effecting data access to the storage device at any particular point in time; and

10 imposing and continuously maintaining the requisite level of data access to said security partition for users effecting said data access in accordance with the particular data access profile thereof regardless of the subsequent operations of the host CPU.

Preferably, the method includes authenticating a user of the computer having a prescribed data access profile and configuring blocking of data access to the storage device to control subsequent access to the security partition in
15 accordance with the data access profile of that user, before that user is able to access said security partition regardless of the particular data access profile of that user.

Preferably, said selective blocking comprises controlling access between the host CPU and the security partition independently of the host CPU.

20 Preferably, said selective blocking occurs during initialisation of the computer and includes intercepting all said data access during the start up sequence immediately after said initialisation and before loading of the operating system of the computer to enable independent control of the host CPU and configuration of the computer in a manner so as to prevent unauthorised access to the storage
25 device.

Preferably, the method includes performing a software boot of the computer after correct authentication of the user, and allowing normal loading of the operating system during the start up sequence of the computer thereafter.

- 8 -

Preferably, the method includes controlling blocking access to the storage device after correct authentication of the user in accordance with the prescribed profile of access of the user.

Preferably, the method includes unalterably storing computer programs for
5 effecting said controlling access in a location separate from the memory and not addressable by the host CPU.

Preferably, said authenticating includes enabling a user of the computer to enter a login identification and password and verifying the same to establish whether the user is an authorised user of the computer having a prescribed profile of access to
10 the storage device before allowing the start up sequence of the computer to proceed further.

Preferably, said login identification and passwords of authorised users and the prescribed profile of access thereof form part of said critical data and control elements and the verifying includes comparing the entered login identification and
15 password with the login identification and passwords within said critical data and control elements and authenticating a user if there is match.

Preferably, the prescribed profile of access comprises a prescribed allocation of predetermined levels of access permitted for an authorised user to prescribed partitions of the storage device. Preferably, the prescribed partitions include the
20 security partition.

Brief Description of the Drawings

The accompanying drawings, which are referred to in the following description of the Best Mode for Carrying Out the Invention, are briefly described as follows:-

Figure 1 is a schematic box diagram of a typical computer system showing the
25 physical location of the security device relative to the host CPU, main bus, interface logic and various peripheral devices in accordance with the first embodiment;

- 9 -

Figure 2 is a schematic box diagram of the security device showing its general functional make-up in accordance with the first embodiment;

Figure 3 is a flow chart showing the start up sequence of a normal computer that is not equipped with the security device;

- 5 Figures 4A and 4B are flow charts showing the start up sequence of a computer system equipped with the security device as described in accordance with the first embodiment;

Figure 5 is a flow chart showing the various states of operation of the security device from power on in accordance with the first embodiment;

- 10 Figure 6 is a flow chart showing the various processes performed by the authentication application program in accordance with the first embodiment;

Figure 7A shows the graphical specification format of the general login graphical user interface (GUI) screen in accordance with the first embodiment;

- Figure 7B shows the graphical specification format of the normal user type login
15 GUI screen in accordance with the first embodiment;

Figure 7C shows the graphical specification format of the administrator type login GUI screen in accordance with the first embodiment;

Figure 7D shows the graphical specification format of the administrator's user edit GUI screen in accordance with the first embodiment;

- 20 Figure 7E shows the specification format for the administrator's access edit GUI screen in accordance with the first embodiment;

Figure 8 is a schematic box diagram of a typical computer system having bus bridge architecture comprising multiple buses and bus bridge circuits in accordance with the second embodiment;

- 10 -

Figure 9 is a schematic box diagram of a bus bridge circuit according to the second embodiment of the present invention within a computer system of the type shown in Figure 8; and

Figure 10 is a schematic box diagram of a bus bridge circuit according to a third
5 embodiment of the invention.

Best Mode for Carrying Out the Invention

The best mode for carrying out the invention will now be described with respect to several embodiments.

The first embodiment is directed towards a security system for an operating
10 system of a computer of a type that is disclosed in WO 03/003242 by this applicant, which is incorporated herein by reference. The security system includes the formation of a security partition where the operating system of the computer is stored, and which is configured in a manner so as to protect the operating system during operation of the computer.

15 As shown in Figure 1 of the drawings, the computer system 11, within which the security system is connected, generally comprises a central processing unit (CPU) 13 and a plurality of peripheral devices, which are connected via a main CPU address and data bus 15. The peripheral devices include a monitor 17, a keyboard 19 and one or more read/writeable storage devices 21. In the present
20 embodiment, the storage devices 21 communicate according to the ATA (AT attachment) standard and thus require an ATA channel to be provided between them and the remainder of the computer system 11.

These peripheral devices are connected to the main CPU bus 15 via appropriate interface logic 23, 27 and 31, each comprising decode logic and device I/O
25 (input/output). The interface logic is characterised to allow communication between the CPU 13 and the particular peripheral device.

- 11 -

In the case of the monitor 17, the interface logic 23 therefor is integrated with a video adapter and is connected via a standard video cable 25 to the monitor; in the case of the keyboard 19, the interface logic 27 therefor is integrated with a keyboard port and is connected via an appropriate keyboard cable 29 to the
5 keyboard; and in the case of the storage device(s) 21, the interface logic 31 therefor is integrated with an ATA adapter and is connected via an ATA cable 33 to the storage device(s) to provide the ATA channel.

The security system of the present embodiment includes a discrete security device 35 physically interposed inline with the ATA cable 33 between the ATA
10 adapter provided on the device interface logic 31 and the storage devices 21. The ATA standard supports most types of storage device, including hard disk drives, CD-ROMS (which actually adopts the ATA/ATAPI enhancement to the ATA standard), flash memory, floppy drives, zip drives and tape drives.

Under the ATA standard, two discrete storage devices may be controlled via the
15 single interface logic 31 and ATA cable 33. Hence reference will be made hereinafter to "storage media", which will comprise either one or two storage devices, and will be used interchangeably with "storage device".

In the case of PCs, the main type of read/writeable storage device is the HDD. Most HDDs conform to the IDE (Integrated Drive Electronics) hard drive standard
20 or the EIDE (Enhanced IDE) hard drive standard, whereby the controller for the disk drive is located on the HDD itself as opposed to being directly connected to the motherboard of the PC.

Although not shown in the drawings, other embodiments of the computer system may involve storage media connected to the main computer system via a SCSI
25 (Small Computer Systems Interface) standard, which has its own corresponding interface logic. In the case of storage media connected to the PC in this manner, the security device 35 would similarly be interposed between the SCSI drive device and the interface logic thereof.

- 12 -

The security system also includes a security partition 36, which is logically configured as a discrete partition on one of the storage devices. Importantly, the operating system of the computer is stored in the security partition 36.

In the present embodiment, the security partition 36 is C: (C drive), and takes up a
5 portion of the entire disk space that is available on the storage media 21. Thus the storage media 21 is formatted with a plurality of partitions, such as C:, D:, E: and F:.

As shown in Figure 2 of the drawings, the security device 35 generally comprises a CPU 37, RAM (random access memory) 39, flash ROM (read only memory) 41
10 and bus control and interface logic 43, which in the present embodiment is adapted to the ATA standard for the purposes of protecting the ATA storage media 21. The bus control and interface logic 43 is typically embodied in FPGA (Field Programmable Gate Array) and/or ASIC (Application Specific Integrated Circuit) devices that are connected so as to intercept and permit control of all
15 communications between the host CPU 13 and the disk storage media 21 under the control of the security device CPU 37.

The security device 35 also includes a secure media interface 45 that allows a separate secure storage media 47 to be connected to the security device via a custom interface 49.

20 The security device CPU 37 operates according to a prescribed application program stored in the flash ROM 41 and which is loaded into the RAM 39 on start up and becomes the operating system for the security device. The CPU 37 communicates with the bus control and interface logic 43, which is interposed in line with the ATA cable 33 to function as blocking means that intercepts
25 communications between the host CPU 13 and the storage media 21. The secure media interface 45 is interposed between the bus control and interface logic 43 and the custom interface 49 to facilitate communications between the host CPU 13 and the secure storage media 47 under the control of the CPU 37.

- 13 -

The functionality of the application program stored in flash ROM 41 and the operation of the security device 35 will now be described with reference to Figures 3 to 5.

The application program stored in flash ROM 41 for the security device 35 is
5 generally designed to intercept and control the computer system's boot process and provide authentication by means of a login ID and password before access to the protected storage media is permitted. Further, the location of the security device 35 between the host CPU 13 and the storage media 21 is particularly designed so that the security device is able to filter all requests for information and
10 data flowing to and from the storage media. The security device 35 forwards these requests to the storage media as appropriate, based on predetermined user profiles that are set up by a user having an administrator profile, which profiles are stored within the security device itself. These profiles are based on access to different partitions and/or files within the storage media. Thus the designated
15 administrator can set up data protection on a partition-by-partition and/or file-by-file basis and so can set up data protection for the operating system in a specific security partition in a manner that will be described in more detail later.

Once the security partition is set up containing the operating system, the security device can interact with the operating system as a pseudo host CPU and allow
20 the operating system to function normally, whilst shielding it from any malicious or unauthorised operations that may take control of the normal host CPU of the computer, without the knowledge of the user.

In order to fully understand the operation of the security system and how it protects the operating system, an appreciation is required of the normal boot
25 process followed by a standard computer system. This boot process will now be described with reference to Figure 3 of the drawings.

As shown in Figure 3, the normal start up sequence followed by a PC commences as indicated at step 51 with power on shown at 53. This is also known as a "cold" boot, whereby all left over data from the host CPU's internal memory registers and
30 RAM is cleared and the program counter of the CPU is set with the starting

- 14 -

address to commence the boot process. This address is the beginning of a boot program stored permanently in the ROM BIOS (Basic Input Output System).

The next step 55 involves the CPU using the address to find and invoke the ROM BIOS boot program. The ROM BIOS program goes through an initialisation phase
5 that includes setting up hardware and software interrupt vectors and invoking a series of system checks known as power-on self-tests (POSTs) as represented by step 57.

The POST process involves a series of tests to ensure that the RAM of the PC is functioning properly. It then conducts another series of tests, which instruct the
10 host CPU to check that the various peripheral devices, such as the video card and monitor 17, keyboard 19 and storage media 21, are present and functioning properly.

On completing the POST, the BIOS then looks for addresses of BIOS extensions at step 59 that are held in the ROMs of peripheral devices to see if any of them
15 have an extended BIOS to run.

The first of these BIOS extensions is associated with the video card. This BIOS extension initialises the video card to operate the monitor as shown at step 61.

Upon completing initialisation of the video card, the BIOS then proceeds at step 63 to run other BIOS extensions for those peripheral devices that have them.

20 The BIOS then proceeds to display the start up screen at step 65, before proceeding with conducting further tests on the system at step 67, including the memory test at step 67, which is displayed on the screen.

The BIOS then performs a "system inventory" or equipment check to determine what type of peripheral hardware is connected to the system at step 69. With
25 respect to HDD storage media, the BIOS program causes the host CPU to interrogate the HDD requesting details such as the drive standard (ATA or SCSI), which level of standard (eg whether it is the old standard ATA 1-3 or the new

- 15 -

standard ATA 6) the number of cylinders/heads/sectors, and whether it is capable of running in other modes. This stage of interrogation of the HDD is known as "drive ID".

The BIOS then proceeds to configure "logical" devices, such as Plug and Play
5 devices, at step 71 and displays a message on the screen for each one it finds.

The summary screen is then displayed at step 73 indicating the configuration of the computer system. The BIOS then checks for the specified boot sequence at step 75, where the order of priority of storage media to be checked for the location of a valid boot sector, from which the operating system of the computer may be
10 loaded, is specified. The normal order is to check the floppy disk drive (A:), then the hard disk (C:) or vice versa, or the CD ROM drive.

Having identified the order of priority, the BIOS causes the CPU at step 77 to look for boot information in each drive in sequence until a valid boot sector is located.

The BIOS undertakes this process by invoking the software interrupt vector "int 19
15 at step 79, which stores the address of the particular peripheral device in a software interrupt vector table that is set up during the initialisation phase of the BIOS.

For example, if the target boot drive is the HDD, the CPU looks for a master boot record or boot sector at cylinder 0, head 0, sector 1 (the first sector on the disk), at
20 the address of the device specified in the table: if it is searching a floppy disk, it obtains the address of the floppy disk drive from the table and looks for a volume boot sector at the same location on the floppy disk.

A valid boot sector is determined by the CPU checking the signature of the "ID byte", which normally comprises the first two bytes of the boot sector. If the
25 signature signifies that a boot sector is present, the CPU then proceeds with loading the boot sector at step 81 into RAM and executes or runs the boot loader at step 83 for loading the various operating system files.

- 16 -

In the case of the DOS operating system, the hidden files MS DOS.SYS, IO.SYS and COMMAND.COM are loaded and executed and then the files CONFIG.SYS and AUTOEXEC.BAT are loaded and run to complete configuration of the computer system and allowing appropriate application programs to be initiated for subsequent operation of the computer system.

In the case of the embodiment of the present invention incorporating the security device 35, the security device is programmed to block out all access of the host CPU 13 to the protected storage media 21 by intercepting the boot process at an early stage during operation of the BIOS. In addition, the security device provides for a custom boot sector to be loaded into the RAM of the host CPU 13, which then executes an authentication application program requiring correct user authentication before allowing the computer system to proceed with its normal boot sector operation and operating system loading. Since the latter operations require access to the protected storage media 21, this methodology ensures that such access is undertaken only after the supervisory control of the security device 35 has been established on a user-by-user basis.

This manner of operation of the security device 35 is best explained in conjunction with Figures 4A, 4B and 5 of the drawings, which outline the operation of the computer system start up sequence with the security device installed in the manner previously described.

In this arrangement, the cold boot process of the computer system commences with the start and power on steps 51 and 53, as in the case of the normal computer start up sequence. At power on, however, the security device 35, which is separately powered, undergoes its own initialisation phase commencing with the start step 100, whereupon all of its onboard resources are initialised at step 101 and its operating system program is loaded and run to enter its first phase of operation as shown at step 102. The initialisation phase of the security device 35 should proceed far more quickly than it takes the BIOS of the computer system 11 to initialise, due to the reduced overheads of the security device as compared with those of the computer system. Accordingly, the operating system program stored in flash ROM 41 immediately invokes the

- 17 -

security device CPU 37 at step 103 to control the bus control and interface logic 43 and intercept all communications from the host CPU 13 to the storage media along the ATA channel, so that no communications are allowed between the host and the protected storage media 21 along the ATA cable at all during this time.

- 5 Prior to this time the bus control and interface logic 43 is not configured and so no access to the storage media is available prior to or during the initialisation phase of the security device along the ATA cable, in any event.

- The security device CPU 33 then places a drive busy signal on the ATA channel to inform the host CPU 13 of the status of the storage media 21 and proceeds
10 with requesting the "drive ID" from the storage media, as shown at step 104.

The operations of the security device 35 during this time occur quite independently of the BIOS, whereby the BIOS proceeds with performing steps 55 through to 69, in accordance with its normal operation, until the "drive ID" check is performed by it at step 69.

- 15 During steps 55 to 69, the security device 35 continues to block of all data communications from the host CPU 13, or any other external device, with the storage media 21. During this "drive busy" phase, the CPU 37 of the security device 35 is in a state waiting for the "drive ID" information from the storage device. Once the security device CPU 37 receives the "drive ID" information from
20 the storage media 21, the CPU 37 stores this in its RAM 39 and asserts a "drive ready" signal on the ATA channel to indicate to the host CPU 13 that the storage media 21 is ready to provide the "drive ID".

- If the host CPU 13 has already reached the "drive ID" stage 69 and has been polling the drive interface logic 31 during the "drive busy" phase for less than the
25 requisite time period, or more normally when the BIOS finally reaches the "drive ID" stage at step 69 after the security device CPU 37 has signalled the "drive ready" phase on the ATA channel, the host CPU 13 issues a request to the driver interface logic 31 of the "drive ID".

- 18 -

Once this request is made at step 69, the security device CPU 37 intercepts the request at 105, continuing to block access to the storage media 21, and provides the host CPU 13 with the "drive ID" of the HDD(s) at step 106.

The BIOS provides for a thirty one second period for the HDD to respond with the "drive ID" information stored describing it. Accordingly if the security device CPU 37 is not able to provide the "drive ID" information within this time, from the time that the BIOS reaches the "drive ID" equipment check stage 69, for whatever reason, then the BIOS will indicate that the storage media 21 at that location is not functional and bypass it. As the security device 35 is expected to be well and truly initialised and operational by this time, such a delay would generally be indicative that there is indeed a problem with the protected HDD(s).

After supplying the host CPU 13 with the "drive ID", the security device 35 advances to its next state, still blocking data communications between the host CPU 13 and the protected storage media 21, whilst the BIOS program proceeds with its normal boot up procedure at steps 71 through to 81, until it arrives at step 81 involving loading of a valid boot sector.

During this state, the CPU 37 of the security device 35 waits for a boot sector request from the host CPU 13 to the driver interface logic 31. On receiving the BIOS request, instead of loading the boot sector stored on the protected storage device, the security device supplies a "custom" boot sector stored on its own flash ROM 41 to the host CPU as indicated by step 107. The CPU 13 then runs the boot loader according to the custom boot sector, which causes a prescribed authentication application program stored within the flash ROM 41 to be loaded at step 109 and then executed at step 111.

In the present embodiment, the valid boot sector must be that which is stored on the protected storage media 21; otherwise the security device 35 never advances beyond its blocking state. Such an arrangement ensures the integrity of the security of the system by not allowing any external operating system, other than that which is provided on the protected storage media 21, to effect control of the

- 19 -

host CPU 13 for the purposes of communicating with data stored on the protected storage media 21.

Thus, in the normal operation of the computer system, where the BIOS targets the protected storage media 21 for the purposes of locating and loading the boot sector, the BIOS causes the host CPU 13 to request the boot sector from the
5 protected storage media 21.

The authentication application program combines with the host CPU 13 to provide profiling means that essentially comprises a prescribed login application that only allows an authenticated user to continue with operation of the computer system
10 11. A user that is unable to be authenticated by the prescribed login application cannot continue to use the computer system. The detailed operation of the login application will be described in more detail later, but for the purpose of describing the system start up sequence, will be described in general terms.

Moreover, the login application requires the user to enter a valid login name and
15 password for the computer system to progress beyond the initial login stage. The login application in the present embodiment is designed to allow only three attempts at entering the correct login name and password. It should be appreciated that in other embodiments the number of login attempts that may be allowed can be different, and in extreme security applications, may be limited to
20 just one attempt. If the correct login name and password are not entered by the third attempt, the application program invokes a system halt (wherein the system hangs or loops indefinitely), which requires the entire cold boot process to be repeated.

Valid login names and passwords associated therewith for all users permitted
25 access to the storage media 21 are stored in the flash ROM 41 of the security device 35. Accordingly, various communications proceed during this login phase between host CPU 13 under the control of the authentication application program and the security device CPU 37 as shown at 112.

- 20 -

If the login is successful, as represented by step 113, the authentication application program proceeds in a manner to be described in more detail later. With respect to the security device 35, once the user has been authenticated, the data access profile previously stored for that particular user in the flash ROM 41 is
5 set at 114 to determine the protocol of operation between the authentication application program and the operating system of the security device thereafter. During this phase of operation, the security device CPU 37 passes details of the data access profile of the particular user to the host CPU 13 for display. Depending upon the access level of the user, possibly login and password
10 information as well as data access profile information of other users having access to the storage media 21 are passed over to the host CPU for display and possible editing under the authentication application program.

This phase of operation continues until the user invokes an "allow boot" process at step 115. Setting this status causes the security device 35 to enter the second
15 phase of its operation at step 117. At this stage, the operating system being run by the security device CPU 37 configures the security device 35 to set the data access profile of the authenticated user at step 119, which profile is thereafter enforced for determining the host CPU 13 access to the protected data storage media 21.

20 The operating system of the security device 37 then signals the authentication application program run by the host CPU 13 at 120 that the security device bus control and interface logic 43 is configured to adopt the data access profile of the user, whereupon the application program at 121 issues the software interrupt vector to the host CPU 13 invoking a "warm boot". The appropriate soft boot
25 vector is then loaded and the host CPU 13 causes a soft system re-start or warm boot at step 85.

During the software reset, the security device 35 then enters a waiting state for the boot sector request as indicated at 123, whilst enforcing the data access profile for all data communications between the host CPU 13 and the protected
30 storage media 21 as shown at 125. Importantly, whilst the computer system 11 is

- 21 -

undergoing the system reset, its security device 35 still remains active and fully operational during this time.

A software reset "warm boot" invokes a special subroutine of the BIOS program that performs an abbreviated start up sequence. Moreover, essentially steps 51
5 to 63 are bypassed and the BIOS program proceeds with operation at about step 65.

At step 69, which invokes the equipment check involving the "drive ID" with respect to the HDD, the operating system of the security device 35 no longer intercepts the request from the host CPU 13 to the protected storage media 21, as
10 long as the access to the HDD of the storage media is in conformance with the particular user data access profile that has been set by the operation of the security device 35 during the first phase of its operation. Such access will be permitted in most cases, unless the administrator has specifically barred the authenticated user from HDD access.

15 Thus, the security device 35 allows the HDD of the storage media 21 to respond directly to the request with the "drive ID", whereupon the host CPU 13 advances the BIOS program through steps 71 to 81, in accordance with the normal boot up sequence of the BIOS.

Importantly, the initial part of the data access profile enforcement process involves
20 the operating system of the security device 35 blocking access to the protected storage media 21 until a valid BIOS boot sector request is detected from the host CPU 13 via the ATA cable 33. Importantly, the security device CPU 37 rejects all other commands to the protected storage media during step 125.

On the BIOS requesting a boot sector from the particular HDD of the protected
25 storage media 21, the bus control and interface logic 43 of the security device allows the request to proceed.

On the BIOS receiving a valid signature from the storage media, the host CPU 13 then proceeds with loading the prescribed boot sector from the storage media 21

- 22 -

at step 81 and proceeds running the boot loader to load the operating system from the storage media 21 at step 83, in accordance with the normal operation of the computer system.

Following receipt of a valid BIOS request for the boot sector on the storage media
5 21, the security device 35 then adopts a monitoring state of all media channel activity along the ATA cable 33 and configures the bus control and interface logic 43 of the security device according to the set data access profile of the authenticated user as indicated at 127. Accordingly, the security device 35 only allows or disallows access to relevant partitions and files within the storage media
10 21 in conformance with the set user data access profile, whereby data that the user is not permitted to access cannot be accessed by the user or by any virus, errant application program or unauthorised access.

The security device 35 maintains this monitoring or supervisory state until the computer system 11 is shutdown and powered off. Once power is switched off to
15 the security device, all dynamic memory is erased and access to the storage media is barred until the device is powered up and initialised again.

Now having described the general operation of the security device 35, the authentication application program will now be described in more detail with respect to the flow chart shown in Figure 6 and the GUI screen graphical
20 specification formats as shown in Figures 7A through to 7E.

The user authentication application program, on being loaded by the boot loader at step 109 and run by the host CPU at step 111, commences at 130 and initially causes a user login screen to be displayed at step 131, the graphical specification for which is shown at Figure 7A of the drawings. The screen 132 is divided into a
25 heading frame 133, a login frame 135 and a message/log frame 137.

The heading frame 133 has provision for the product trade mark at 139, the version number at 141, the screen name at 143 and provision for display of legal warning notices at 145.

- 23 -

The login frame 135 includes banners for the text "user:" at 147 and the text "password:" 149, with frames for respectively entering the user identification or "user ID" at 151 and the user password at 153. The message/log frame comprises a banner for displaying the text "messages" at 157 and a message
5 frame 159, which displays status messages issued by the security device to the authentication application program as a scrollable list. A login button 155 is also provided in order for the user to invoke the processing of the user and password entries for authentication purposes by the security device.

Whilst the screen 132 is displayed, the application program waits for the login ID
10 and password to be entered as shown at step 160. Activating the login button 155 involves the authentication application program invoking a process at 161 causing the host CPU 13 to pass the login details entered on the screen to the security device 35, whereupon the operating system of the security device causes the security device CPU 37 to compare the received login information with stored
15 login information provided in the flash ROM 41. Depending upon whether there is a valid match between the entered user and password information via the login screen and the stored user and password information, the security device CPU 37 returns either a valid or invalid authentication signal to the host CPU 13.

In the case of there being a valid authentication as shown at 162, the CPU 37 also
20 provides additional information concerning the user type and associated device information depending upon the stored data access profile of the particular user.

In the case of there being an invalid authentication, a counter is incremented/decremented to record that a first unsuccessful attempt at authentication has been made and an appropriate message is displayed to the
25 user on the message/log frame 137, indicating the failed status of the authentication attempt as shown at 163. As previously described, on three unsuccessful authentication attempts as shown at 164, the authentication application program causes a shutdown interrupt vector to be invoked by the host CPU 13 at 165, resulting in a complete shutdown of the computer system 11
30 requiring a cold boot to restart the system.

- 24 -

On valid authentication, the authentication application program then proceeds at 166 with displaying one of either two types of login screen, depending upon the user type. In the present embodiment, there are two user types, one being a normal user, for which the screen as shown by the graphical specification at
5 Figure 7B is displayed at step 167, and the other being an administrator for which the screen represented by the graphical specification at Figure 7C is displayed at step 168.

The graphical specification for the normal user GUI screen 169 is generally divided into a heading frame 170, a login details frame 171, a device details frame
10 172 and a message/log frame 173. The screen also includes a launch system button 174 that will be further described.

The heading frame 170 is essentially the same as the heading frame 133 for the general login screen, where the same reference numerals have been used to identify corresponding attributes of the frame. In this case, however, the screen
15 title is modified to represent that it is a user type login screen, as shown at 143 of the drawings.

The login details frame 171 is similar to the login frame 147 of the preceding screen and accordingly the same reference numerals have been used to identify corresponding attributes of the frame. The login details frame, however, includes
20 a user ID display frame 175 to display the user ID as opposed to an entry frame in the proceeding screen. The login details frame also includes a new password accept button 176, which is used in conjunction with the password entry frame 153 to permit the user to change its password. Accordingly, activating the new password button 176 invokes a process within the authentication application
25 program involving communication between the host CPU 13 and the security device CPU 37 to cause a change to the password stored within the flash ROM 41 of the security device for the particular user as shown at 177. A standard routine involving confirmation of the new password is adopted, before the password changes are completed.

- 25 -

The device details frame 172 includes a title banner 178, which displays the text "device information", as well as two further sub-banners displaying the text "master" at 179 and "slave" at 181. These sub-banners head regions for displaying information about the prescribed device or devices that are protected by the security device 35. In the present embodiment, up to two storage devices are allowed, which is normal under the ATA standard, one being denoted the "master" device and the other being denoted the "slave" device. The respective regions detailing the device information include three further sub-level banners for displaying the text "device" at 183, "access" at 185 and "size MB" at 187. Display frames 189 for each sub-banner are respectively provided below the device, access and size banners for listing the device details that the user is permitted to observe on the master and/or slave device, as set by the administrator.

For each observable device, the list displays:

- the device number;
- its access type for the user: and
- the device size in MB (MegaBytes).

The access type lists one of five possible designations:

- read only, which is displayed in red text;
- read/write, which is displayed in green text;
- invisible, which is displayed in yellow text;
- read directory entry, which is displayed in grey text; and
- delete, which is displayed in blue text.

The message/log frame 173 includes a title banner 157 for displaying the text "messages" and a display frame 159, which displays status messages provided by the security device as a scrollable list, similar to the preceding screen.

In the case of the user, the device information is only provided for display purposes and cannot be changed.

- 26 -

Now explaining the methodology behind the listings contained in the display frames 189 and the action provided thereby in more detail, in the present embodiment, the protected storage device is divided into partitions that have different access level permissions depending upon the determination of the administrator of the computer system 11. These partitions can be created in a known manner and are represented as separate devices for each type of storage device. As previously mentioned, in the present embodiment, these partitions may comprise C:, D:, E: and F:. Thus, each user can have one of five types of access to these partitions, namely read only, read/write, invisible, read directory entry and delete.

Read only access means that the user can access all of the files existing in the designated partition, but can only read the file contents. The user has no write or delete permissions with respect to the files in that partition.

Read/write access means that the user can access all of the files existing in the designated partition and perform both read and write functions with respect to the file contents, but has no delete permissions with respect to those files.

Invisible access means that none of the files within the designated partition are accessible to the user in any form and are hidden, even to the extent that no file details can be listed or be visible at all in any directory listing of files for that partition available to the user.

Read directory entry access means that the user may be able to list file details such as names and attributes in any directory listing of files in the designated partition, but the user has no read, write or delete permissions in relation to any of the files in that partition.

Delete access is the highest level of access to any files within a designated partition, whereby the user not only has full read and write permissions, but also delete permissions in relation to all of the files in that partition.

- 27 -

When the user is ready to continue on with operation of the computer system 11, the launch system button 174 is activated as shown at 190, whereupon the authentication application program sends a signal to the security device 35 to set the "allow boot" status therein as by step 191. Setting the "allow boot" status
5 invokes the commencement of the second phase of operation of the security device 35, as shown at step 117, allowing the system start up sequence to continue with the authentication application issuing a "warm boot" interrupt vector as step 120 in the manner as previously described. This halts the operation of the user authentication application program.

10 In the case of the user type being an administrator, the administrator screen as represented by the graphical specification shown in Figure 7C is displayed to the user on the monitor via the authentication application program at step 168. The administrator type screen 192 is substantially similar to the user type screen and so the same reference numerals have been used to identify corresponding
15 attributes between the two screens. Accordingly, the administrator type screen is divided into a similar heading frame 193, login details 195, device details frame 197 and a message/log frame 199.

With respect to the banner title 143 of the heading frame 193, the text is altered to indicate that the screen is for the administrator type login.

20 The device details frame 197 and the message/log frame 199 are substantially identical to the corresponding attributes of the user type screen and will not be described further. The launch system button 174 functions in an identical manner to the launch system button of the preceding screen, whereby activation of the same as shown at 200 invokes the commencement of the second phase of
25 operation of the security device 135 as previously described.

With the login details frame 195, the same facility for changing the password of the administrator is provided as shown at step 201, with a similar entry frame 153 and accept new password button 176, as in the case of the user type login. However, the login details frame also includes an edit users button 202, activation
30 of which invokes an editing process within the authentication application program

- 28 -

as shown at 203, allowing the administrator to create and edit data access profiles for individual users, so as to determine their data access profile for permitted access to the storage media 21. Activation of the button 201 causes the authentication application program to display at 204 an administrator editing
5 screen to the user, the graphical specification of which is shown at Figure 7D of the drawings.

The administrator users edit screen 205 is divided into a heading frame 206, an edit user details frame 207, a message/log frame 209 and a return to admin login button 211. The heading frame 206, apart from having an appropriately worded
10 title banner 143 denoting the screen as being an administrator edit users screen is identical to previous heading frames. Similarly, the message/log frame 209 is substantially identical to the message/log frame with the preceding screens. Thus the same reference numerals have been used to identify corresponding attributes of each of these screens.

15 With respect to the edit users details frame 207, this comprises a title banner depicting the text "user list" as shown at 213 and sub-title banners depicting the text "user" at 215, "password" at 217 and "access" at 219. An editable frame 221 is provided below the sub-banners in which is displayed a scrollable and editable
20 list of all users having access to the protected storage media 21. This list is derived from data stored within the flash ROM 41 of the storage device arising from communications between the host CPU 13, under the control of the authentication application program, and the security device CPU 37, under the control of the operating system thereof.

Each user entry in the list contains:

- 25 •the user ID;
 •password; and
 •access button;

under the respective sub-title banners 215, 217 and 219.

- 29 -

Upon pressing the access button for a particular user, the access edit screen will appear for that user. The administrator editing process allows a user to be deleted by the administrator through the edit frame 221 by selecting their entry and pressing the ALT-d key sequence on the keyboard.

- 5 A create new user button 223 is also included within the edit user details frame 207 for creating a new user. Activation of the button 223 invokes a prescribed process within the authentication application program as shown at 224. This process causes a dialogue box to be displayed over the administrator edit users screen 205 providing for frames for entering the user ID and password, and an
- 10 accept button, whereupon activation of which causes the user and password to be displayed in the edit frame 221 as shown at 225. Each new user has an initial default data access profile, which sets up all partition devices as hidden, until such time as the administrator edits the data access profile for the user using the access edit screen. The administrator accesses this screen by activating the
- 15 corresponding access button as shown at 226 for the user requiring editing in the edit frame 221.

The return to admin login button 211 is provided to allow the administrator to return to the administrator type login screen 191 from the administrator edit users screen 205 as shown at 227.

- 20 Activating the access button beneath the sub-title banner 219 alongside any user listed in the user list of the edit user details frame 207 causes the authentication application program to display at step 228 the administrator access edit screen, the graphical specification of which is shown in Figure 7E of the drawings. The administrator access edit screen 229 is divided into a heading frame 230 and an
- 25 edit access details frame 231, a message/log frame 232 and a return to admin user text edit screen button 233.

The heading frame 230 is the same as in preceding screens except that the title banner is provided with appropriate text to identify that the screen is of the administrator access edit type as shown at 235. The message/log frame 232 is

- 30 -

the same as in proceeding screens and accordingly the same reference numerals have been used to identify corresponding attributes between the screens.

The edit access details frame 231 comprises a head banner 235 displaying the text "access details", a sub-banner 237 containing the text "user" and a display
5 frame 239 adjacent thereto for displaying the user ID of the particular user selected from the administrator edit user screen 205.

The edit access details frame 229 then provides a similar frame set up to the device frames of the user type login screen 169 and the administrator type login screen 192, whereby banners for the "master" and "slave" storage media
10 protected by the security device 35 provided at 179 and 181 and respective sub-title banners 183, 185 and 187 detailing the "device", "access" and "size (MB)" titles respectively are provided for each device.

Device detail frames 239 are provided below each of these sub-title banners similar to the display frames 189 of the device detail frames 172 and 197 of the
15 user login and administrator login screens respectively. The device detail frames 239, however, are editable, whereas the former two were not. Accordingly, each device details frame lists the device number under the sub-title banner 183, the access type for the user under the sub-title banner 185 and the device size in MB under the size (MB) sub-title banner 187.

20 The access type for the user is divided into five types:

- read only, depicted in red text;
- read/write, depicted in green text; and
- invisible, depicted in yellow text;
- read directory entry, depicted in grey text; and
- 25 ◦delete, depicted in blue text.

As in the previous case, the device numbers represent each of the partitions that are created for the particular storage media device. This, together with the size

- 31 -

information, is display only, as determined by the information prescribed for the particular partition stored within the flash ROM 41 of the security device, whereas the access type is editable by highlighting and clicking the displayed entry. In this respect, the displayed entries cycle between read only, read/write, invisible, read
5 directory entry and delete through the graphical user interface by clicking an invisible frame around the displayed text.

In this manner, the access type for each partition can be individually set and edited to create a particular data access profile for the selected user. The particular data access profile created for the user is processed by the
10 authentication application program and supplied to the security device 35 on activating the return to admin user edit screen button 233 as shown at 241. At this time, the display data access profile as determined by the administrator is communicated to the security device CPU 35 by the host CPU 13 and stored within the security device flash ROM 41. The administrator at this stage
15 configures the user profile to only allow read access to the security partition on which the operating system of the computer system 11 is stored, thereby preventing the operating system from unauthorised modification or destruction.

Simultaneously, the authentication application program returns to displaying the administrator edit user screen 205 from which the administrator can select and
20 edit the data access profile of other users in the edit list 207.

In the manner described above, the HDD 21 is configured so that the operating system of the computer 11 is stored in a security partition defined by the administrator. The security partition is configured by the administrator so that, at a minimum, an ordinary user has no write or delete permissions in relation to any
25 of the operating system files therein. This protects the operating system of computer 11 from unauthorised modification or destruction. Optimal protection for the computer's operating system may be provided by configuring the security partition in HDD 21 to be invisible to an ordinary user.

The security partition in HDD 21 is further configured so that the administrator of
30 the computer system 11 can selectively write or delete any of the operating

- 32 -

system files in that partition. This facilitates flexible administrative modification and/or upgrading of the operating system.

During normal operation, there will be times when the operating system will want to update system files contained within the read only security partition. If writes
5 are simply not allowed to this partition, then the operating system will not operate correctly. Thus, the application program of the security device is designed to divert all writes intercepted by the bus control and interface logic 43 to a portion of memory in the flash ROM 41, instead of the read only security partition. In this manner, the computer believes it has updated the required files and continues
10 normal operation. Thus a portion of the flash ROM 41 is used as scratchpad memory and is overwritten each time.

An example of this occurrence is:

- During normal operation a user makes changes to desktop like display attributes, desktop theme, background colour etc.
- 15 • The operating system (OS) implements the changes.
- The OS then saves the changes to the HDD to make the new changes the default at startup.
- If the write to the HDD is not allowed, then the OS stops operating normally.
- Therefore, the SDV diverts all writes to a scratchpad area of the flash ROM
20 instead of the read only security partition of the OS.
- This way the OS implements the change and thinks it has updated the system files and continues normal operation.
- The change the user made is in effect until the computer is turned off.
- On power-up the original OS configuration is loaded.

- 33 -

In Summary:

- User changes desktop background colour for example.
- Background colour changes.
- OS tries to update system files by writing to HDD.
- 5 - System files are in read only OS security partition.
- security device diverts system file write to scratchpad area of flash ROM.
- System continues with colour change in effect.
- User turns off computer.
- When computer is turned on, OS is loaded from read only OS security
10 partition.
- Original OS system files are loaded.
- Background colour is original colour before user changed it.

The second embodiment of the best mode is substantially similar to the preceding embodiment, except it is directed towards a security system of a type where the
15 security device is integrated into the bus bridge circuit interfacing the main CPU bus 15 with the data access channel 33 provided by the ATA cable that is connected to the read/writeable storage device 21. This type of security system is disclosed in International Patent Application PCT/AU2004/000210, which is also incorporated herein by reference.

20 For the purposes of describing the second embodiment, reference will be made specifically to Figures 8 and 9.

- 34 -

As shown in Figure 8 the computer system 11 to which the security system of the present embodiment is integrated with comprises an alternative but generally equivalent architecture to that shown in Figure 1. Moreover, the architecture of the computer system as shown in Figure 8 comprises a plurality of buses
5 interfaced with the main CPU bus 15 via appropriate bridging circuits. The buses include a PCI bus 306 and multiple peripheral buses. The peripheral buses include an ISA bus 302 and an IDE bus (or ATA cable) 33.

The CPU bus 15 connects host CPU 13 to CPU/PCI bridge circuit or north bridge 304. The north bridge 304 is an ASIC that provides bridging between the CPU
10 bus 15 and PCI bus 306. The north bridge 304 also integrates system functions such as controlling communication between the host CPU 13, system memory 308 and AGP (Accelerated Graphics Port) 310.

Similar to the north bridge 304, a south bridge 312 bridging circuit is provided as an ASIC that provides bridging between PCI bus 306 and ISA bus 302 and IDE
15 bus 33. The south bridge 312 also integrates miscellaneous system functions such as counters and activity timers, power management, and various interfaces or controllers to handle communication between devices on the PCI bus 306, ISA bus 302 and IDE bus 33. Connected to the IDE bus 33 is the HDD storage device 21. Other storage media can be similarly connected to the south bridge 312 via
20 the peripheral buses.

Figure 9 is a generalised block diagram showing the present integration of the security system 332 within the south bridge 312 and its connection with the HDD 21 via the IDE bus 33, in more detail. The south bridge 312 includes logic for its conventional bus bridging and system functions including a PCI interface 314, IDE
25 interface 31, USB (Universal Serial Bus) interface 316, ISA interface 318, power management logic 320, keyboard/mouse controller 322 and timer logic 324. The south bridge 312 may also include logic for other miscellaneous system functions.

The south bridge 312 also includes security logic 326 and RAM 328. The security logic 326 is functionally equivalent to the CPU 37 and bus control and interface
30 logic 43 of the security device 35 of WO 03/003242 shown in Figure 1. As

- 35 -

described below in more detail, the security logic 326 can selectively secure accesses between the host CPU 13 and the protected HDD 21.

Similar to the security device 35 of WO 03/003242, the security logic 326 operates according to a prescribed application program which is loaded into RAM 328 on
5 start up and becomes the operating system for security logic 326. The prescribed application program is stored in a partition 330 on the protected HDD 21 itself which is invisible to a user and can only be accessed by a designated administrator. The secure invisible HDD partition 330 is described in more detail below. Alternatively, the application program may be stored in the south bridge
10 312 itself or in a separate secure memory (not shown) connected to the south bridge 312. The functionality of the application program stored in the invisible HDD partition 330 and the operation of the security system 332 is substantially the same as described with respect to the previous embodiment.

The application program stored in the invisible HDD partition for the security logic
15 in the south bridge 312 is generally designed to intercept and control the computer system's boot process and provide authentication by means of a login ID and password before access to the protected storage media is permitted. Accordingly, the location of the security logic 326 in the south bridge 312 between the host CPU 13 and the storage media 21 is particularly designed so that the
20 security logic 326 is able to selectively filter all requests for information and data flowing to and from the protected storage media 21. The security logic 326 forwards these requests to the storage media 21 as appropriate, based on predetermined user profiles that are set up by a user having an administrator profile, which profiles are stored within invisible HDD partition 330. These profiles
25 are based on access to different partitions and/or files within the protected storage media 21. Thus the designated administrator can set up data protection on a partition-by-partition and/or file-by-file basis in the same manner as described with respect to the preceding embodiment. Similar to the application program, the user profiles may alternatively be stored in the south bridge 312 itself or in a
30 separate secure memory connected to the south bridge 312.

- 36 -

The security system of the present embodiment, although designed differently, functions in a substantially identical manner to the operation of the preceding embodiment, and so will not be described in specific detail. Thus, in the case of the security system 332 of the present embodiment, the security logic 326 in the south bridge 312 is programmed to block out all access of the host CPU 13 to the protected storage media 21 by intercepting the boot process at an early stage during operation of the BIOS, as in the case of the preceding embodiment. In addition, the security logic 326 in the south bridge 312 provides for a custom boot sector to be loaded into the RAM 308 of the host CPU 13, which then executes an authentication application program requiring correct user authentication before allowing the computer system to proceed with its normal boot sector operation and operating system loading, in the same manner as the first embodiment. Since the latter operations require access to the protected storage media 21, this methodology ensures that such access is undertaken only after the supervisory control of the security logic 326 in the south bridge 312 has been established on a user-by-user basis.

As in the first embodiment of the present invention, the operating system of the computer 11 is stored in a security partition formed in the HDD 21. The security partition is similarly configured so that, at a minimum, an ordinary user has no write or delete permissions in relation to any of the operating system files therein.

Similarly, the security partition in the HDD 21 is further configured so that the administrator of the computer system 11 can selectively write or delete any of the operating system files in that partition.

As opposed to the first embodiment, however, there is no flash ROM provided in the south bridge. Instead, the security logic 326 makes use of the invisible HDD partition 330 to divert all writes directed by the operating system to system files on the OS security partition to a scratchpad portion of the invisible partition. This portion of the invisible partition is overwritten each time, in a similar manner to the function of the flash ROM in the preceding embodiment.

- 37 -

The third embodiment of the invention is substantially similar to the second embodiment, except that the security system is implemented in a bus bridge integrated circuit (IC) provided on the HDD. This embodiment arises from developments with the serial ATA (SATA) standard for connecting HDD's into
5 computer systems, and is also disclosed in International Patent Application PCT/AU2004/000210, which is similarly incorporated herein by reference for the purposes of describing the third embodiment.

As a consequence of the design of SATA interfaces bus bridge IC's have been developed in the form of a highly integrated System-On-Chip (SOC) device, an
10 example of which has been recently announced by Infineon Technologies. This SOC device integrates a 1.6 Gbit/s read channel core, a 3 Gbit/s native SATA interface, a 16-bit microcontroller, a hard disk controller, embedded memory and a quality monitoring system. Such a device is designed to be incorporated into the control circuit of a HDD, essentially bridging communications between a computer
15 bus using a SATA channel for communicating with a storage device, and the HDD of the storage device.

In the present embodiment, the security system is incorporated into a bus bridge circuit of similar configuration to the SOC device described above and has application software operating the same stored on a HDD to which the bus bridge
20 circuit is connected.

As shown in Figure 10, the bus bridge circuit 351 comprises a CPU 353, having memory RAM 355, a SATA interface 357, a disk controller interface 359 and security logic 361.

As in the preceding embodiment, the security logic 361 of the bus bridge circuit
25 351 is configured to load application software stored on the HDD into RAM 355 to selectively secure accesses between the main computer and the HDD, in conjunction with the normal operation of the disk controller.

The function of the application software is substantially identical to that described in relation to the preceding embodiment except for the fact that the security

- 38 -

system is interfaced with and integrated into the hardware and firmware design of the SOC device to exercise control over disk accesses using the disk controller functionally of the device itself.

Consequently, the operating system of the computer 11 is stored in a security
5 partition formed in the HDD 21. The security partition is configured in a similar manner as in the preceding embodiments, so that an ordinary user has no write or delete permissions in relation to any of the operating system files therein.

As also is the case in the preceding embodiments, the security partition is further
10 configured so that the administrator of the computer system can selectively write or delete any of the operating system files in that partition.

It should be appreciated that the scope of the present invention is not limited to the particular embodiment herein described and that other embodiments of the invention may be envisaged without departing from the scope or spirit of the present invention.

15

The Claims Defining the Invention are as Follows

1. A security system for an operating system of a computer having a host central processing unit (CPU), memory used by the host CPU to load programs in order to operate the computer and a read/writeable storage device for storing
5 data to be handled by the computer, the security system, comprising:

a security partition formed in the storage device, wherein the operating system is stored in the security partition;

profiling means to define at least two different data access profiles with respect to the storage device for users of the computer, one access profile ascribing read/write access to data stored on said security partition, and
10 the other access profile ascribing a blocking level of access that does not permit write access to said security partition; and

blocking means for selectively blocking data access between the host CPU and the security partition in accordance with the particular data access profile defined for a user effecting data access to the storage device at any
15 particular point in time;

wherein said blocking means is independent and separately configurable of said host CPU to impose and continuously maintain the requisite level of data access to said security partition for users effecting said data access in
20 accordance with the particular data access profile thereof regardless of the subsequent operations of the host CPU.

2. A security system as claimed in claim 1, including authentication means to authenticate a user of the computer having a prescribed data access profile and configure said blocking means to control subsequent access to the
25 security partition in accordance with the data access profile of that user, before that user is able to access said security partition regardless of the particular data access profile of that user.

- 40. -

3. A security system as claimed in claim 2, wherein said blocking means includes processing means independent of the host CPU for controlling the operation of said blocking means in response to said authentication means.
4. A security system as claimed in claim 3, wherein said blocking means is
5 configured to block all data access by the host CPU to the storage device before and during initialisation of the security system and includes intercepting means to intercept all said data access immediately after said initialisation and effect data access to the storage device and said security partition under the control of said processing means in accordance with the data access profile of
10 users effecting said data access as authenticated by said authenticating means.
5. A security system as claimed in claim 4, wherein said processing means effects independent control of the host CPU and configuration of the computer in a manner so as to prevent unauthorised access to the storage device, upon
15 said intercepting means intercepting said data access immediately after said initialisation and before loading of the operating system of the computer.
6. A security system as claimed in claim 5, wherein said authentication means enables a software boot of the computer to be effected after correct authentication of the user, and said processing means permits normal loading
20 of the operating system during the start up sequence of the computer following said software boot.
7. A security system as claimed in any one of the preceding claims, including memory store means independent of the memory means and the storage device of the computer to store critical data and control elements associated
25 with the basic operation of the computer and access to the storage device.
8. A security system as claimed in claim 7, wherein said critical data and control elements are supplied to and used by the host CPU for verification of the storage device and operating the computer independently of the storage device during the start up sequence of the computer.

- 41 -

9. A security system as claimed in any one of the preceding claims as dependent on claim 2, wherein the authentication means includes a login verifying means to enable a user of the computer to enter a login identification and password and have that login identification and password verified to authenticate said user being an authorised user of the computer having a prescribed profile of access to the storage device before allowing the start up sequence of the computer to proceed further.
10. A security system as claimed in claim 9, as further dependent on claim 7 or 8, wherein said login identification and passwords of authorised users and the prescribed data access profile thereof form part of said critical data and control elements and said login verifying means accesses said critical data and control elements to effect authentication of a user.
11. A security system as claimed in any one of the preceding claims, wherein the prescribed data access profile of a user comprises a prescribed allocation of predetermined levels of access permitted for an authorised user of the computer to prescribed partitions of the storage device, one of said prescribed partitions including said security partition.
12. A security system as claimed in any one of the preceding claims, wherein said blocking means is physically disposed in line with the data access channel between the host CPU and the storage device.
13. A security system as claimed in claim 12, wherein said blocking means is disposed as part of a bridging circuit effecting communications between the main data and control bus of the host CPU and the data access channel connected to the storage device.
14. A security system as claimed in claim 12, wherein said blocking means is disposed as part of a bridging circuit effecting communications between the data access channel and the storage device.

- 42 -

15. A security system as claimed in claim 12, wherein said blocking means is disposed intermediate the data access channel between the main data and control bus of the host CLU and the storage device.
16. A method for securing and protecting an operating system of a computer from unauthorised access, the computer having a host central processing unit (CPU), a read/writeable storage device for storing data to be handled by the computer, and memory used by the host CPU to load programs in order to operate the computer and storage device, the method comprising:-
- forming a security partition in the storage device, and storing the operating system in the security partition;
- defining at least two different data access profiles with respect to the storage device for users of the computer, one access profile ascribing read/write access to data stored on said security partition, and the other access profile ascribing a blocking level of access that does not permit write access to said security partition;
- selectively blocking all data access between the host CPU and the security partition in accordance with the particular data access profile defined for a user effecting data access to the storage device at any particular point in time; and
- imposing and continuously maintaining the requisite level of data access to said security partition for users effecting said data access in accordance with the particular data access profile thereof regardless of the subsequent operations of the host CPU.
17. A method as claimed in claim 16, including authenticating a user of the computer having a prescribed data access profile and configuring blocking of data access to the storage device to control subsequent access to the security partition in accordance with the data access profile of that user, before that

- 43 -

user is able to access said security partition regardless of the particular data access profile of that user.

18. A method as claimed in claim 16 or 17, wherein said selective blocking comprises controlling access between the host CPU and the security partition
5 independently of the host CPU.

19. A method as claimed in claim 18, wherein said selective blocking comprises totally blocking data access to the storage device by the host CPU during initialisation of the computer and includes intercepting all said data access during the start up sequence immediately after said initialisation and before
10 loading of the operating system of the computer, and effecting data access to the storage device and said security partition in accordance with the data access profile of users effecting said data access on authentication thereof.

20. A method as claimed in claim 19, including performing a software boot of the computer after correct authentication of the user, and allowing normal loading
15 of the operating system during the start up sequence of the computer thereafter.

21. A method as claimed in any one of claims 17 to 20, including controlling blocking access to the storage device after correct authentication of the user in accordance with the prescribed data access profile of the user.

20 22. A method as claimed in any one of claims 16 to 21, including unalterably storing computer programs for effecting said controlling access in a location separate from the memory and not addressable by the host CPU.

23. A method as claimed in any one of the preceding claims as dependent on claim 17, wherein said authenticating includes enabling a user of the computer
25 to enter a login identification and password and verifying the same to establish whether the user is an authorised user of the computer having a prescribed profile of access to the storage device before allowing the start up sequence of the computer to proceed further.

- 44 -

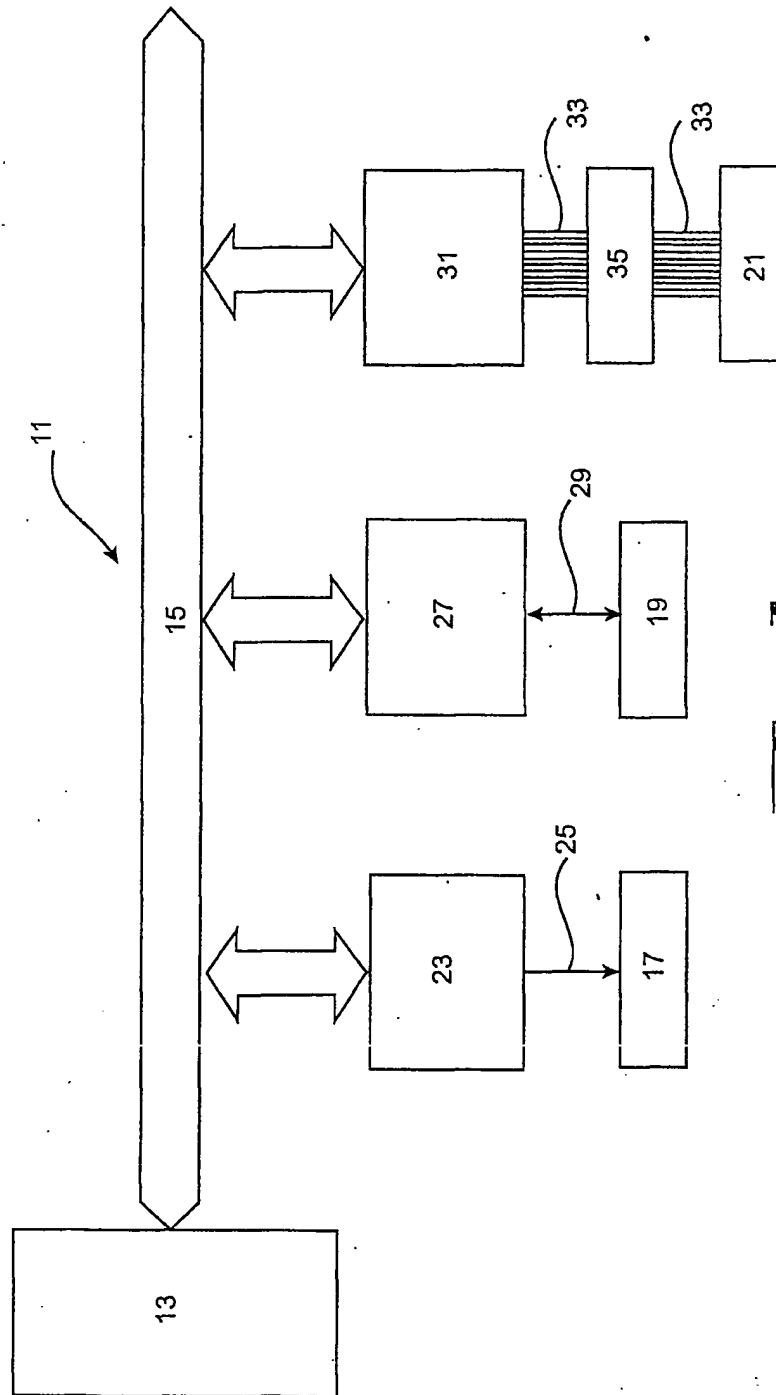
24. A method as claimed in claim 23, wherein said login identification and passwords of authorised users and the prescribed profile of access thereof form part of said critical data and control elements and the verifying includes comparing the entered login identification and password with the login
5 identification and passwords within said critical data and control elements and authenticating a user if there is match.

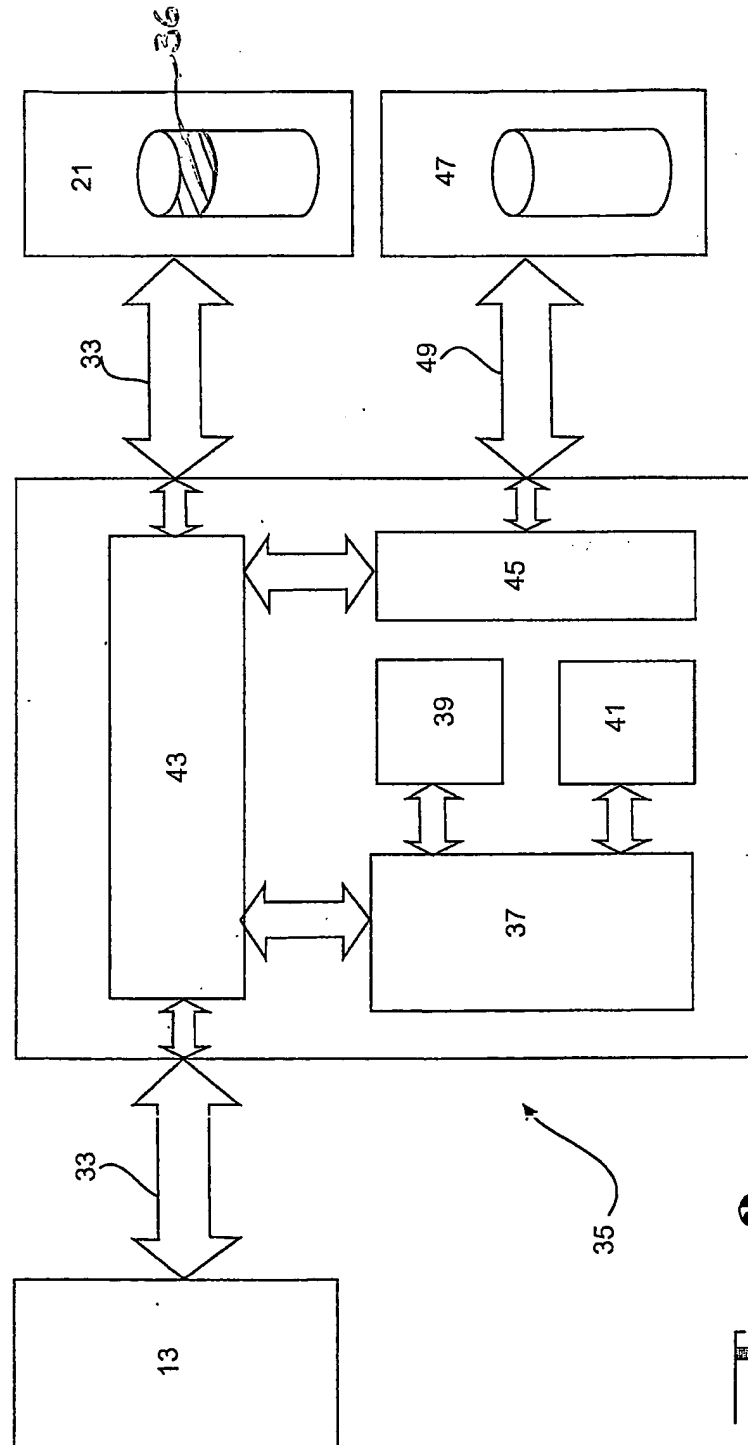
25. A method as claimed in any one of claims 16 to 24, wherein the prescribed profile of access comprises a prescribed allocation of predetermined levels of access permitted for an authorised user to prescribed partitions of the storage
10 device.

26. A method as claimed in claim 25, wherein the prescribed partitions include the security partition.

27. A security system for an operating system of a computer, the security system being substantially as herein described with reference to the accompanying
15 drawings as appropriate.

28. A method for securing and protecting an operating system of a computer from unauthorised access, substantially as herein described with reference to the accompanying drawings as appropriate.





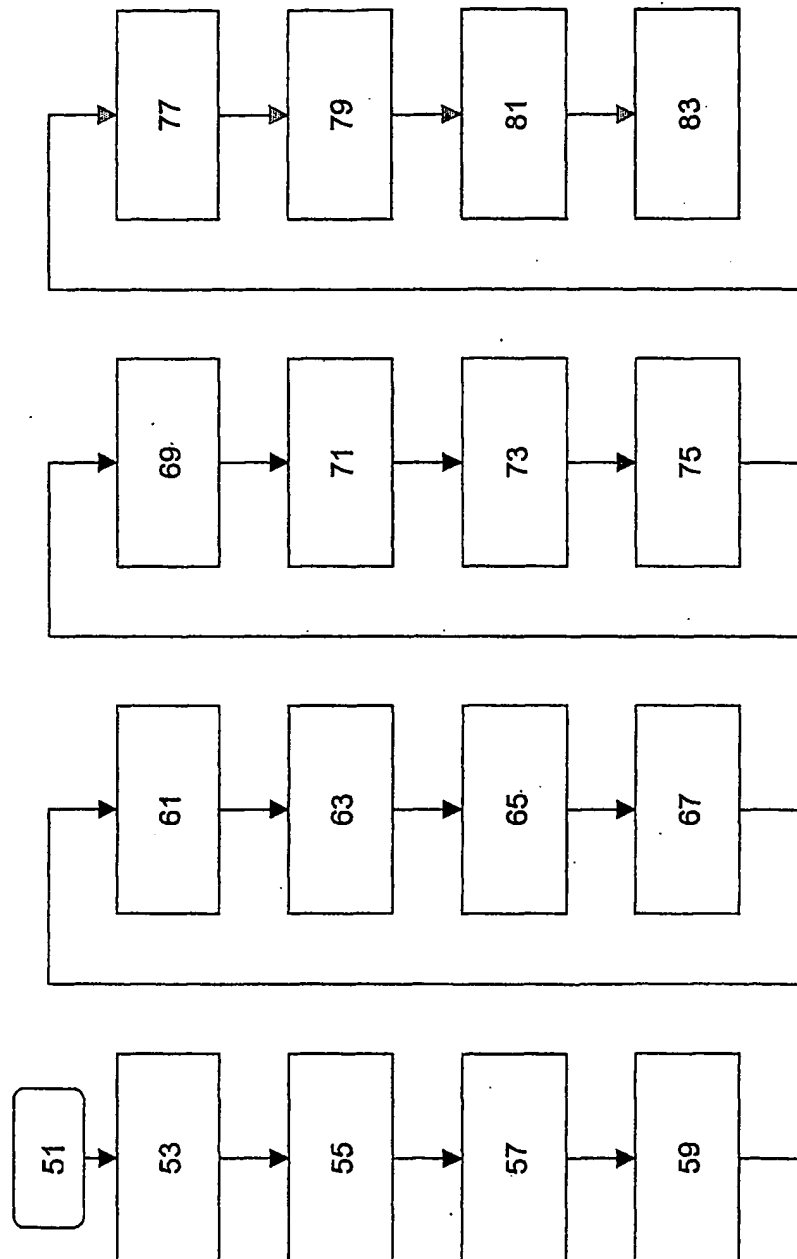


Figure 3

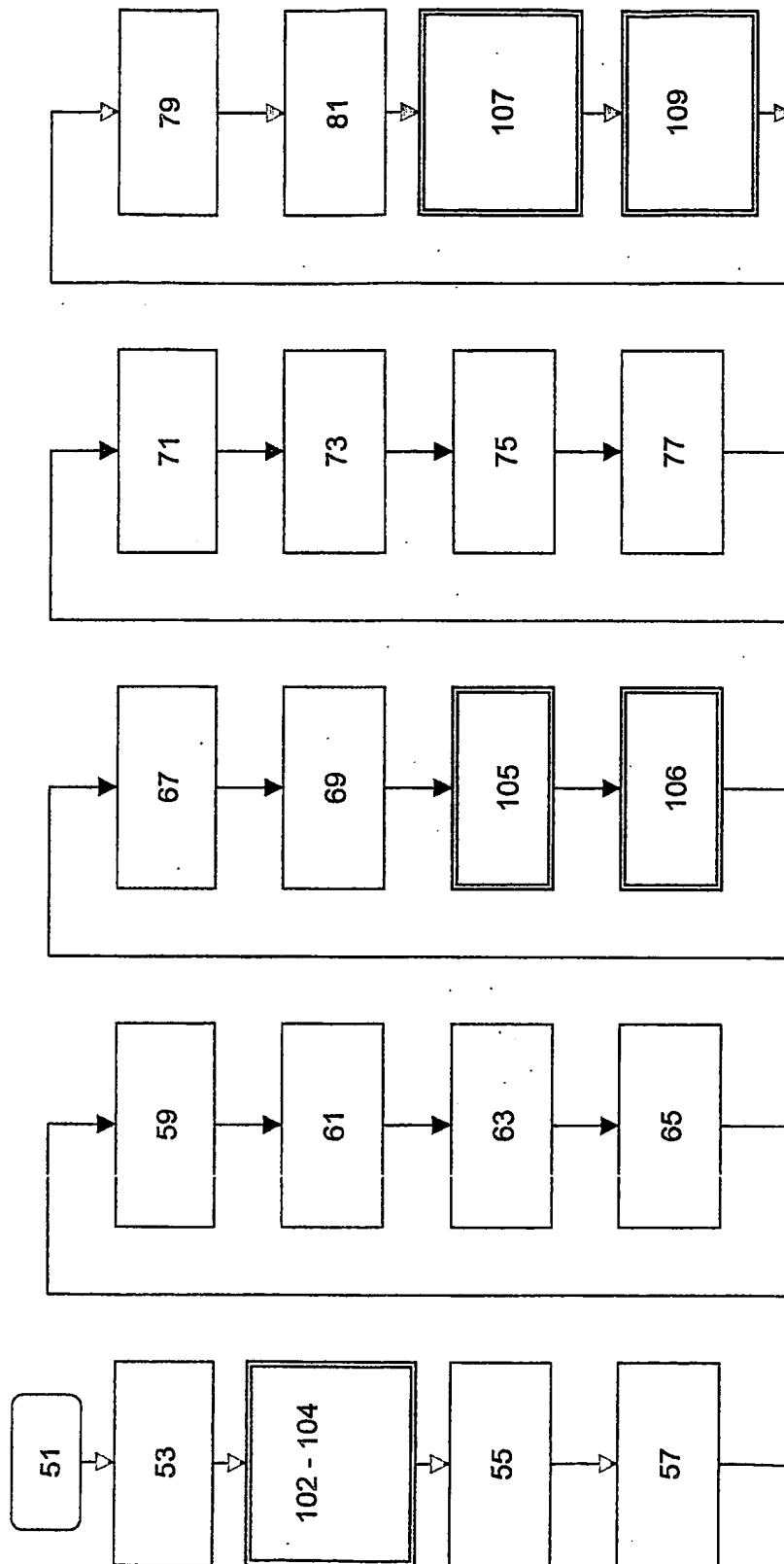


Figure 4A

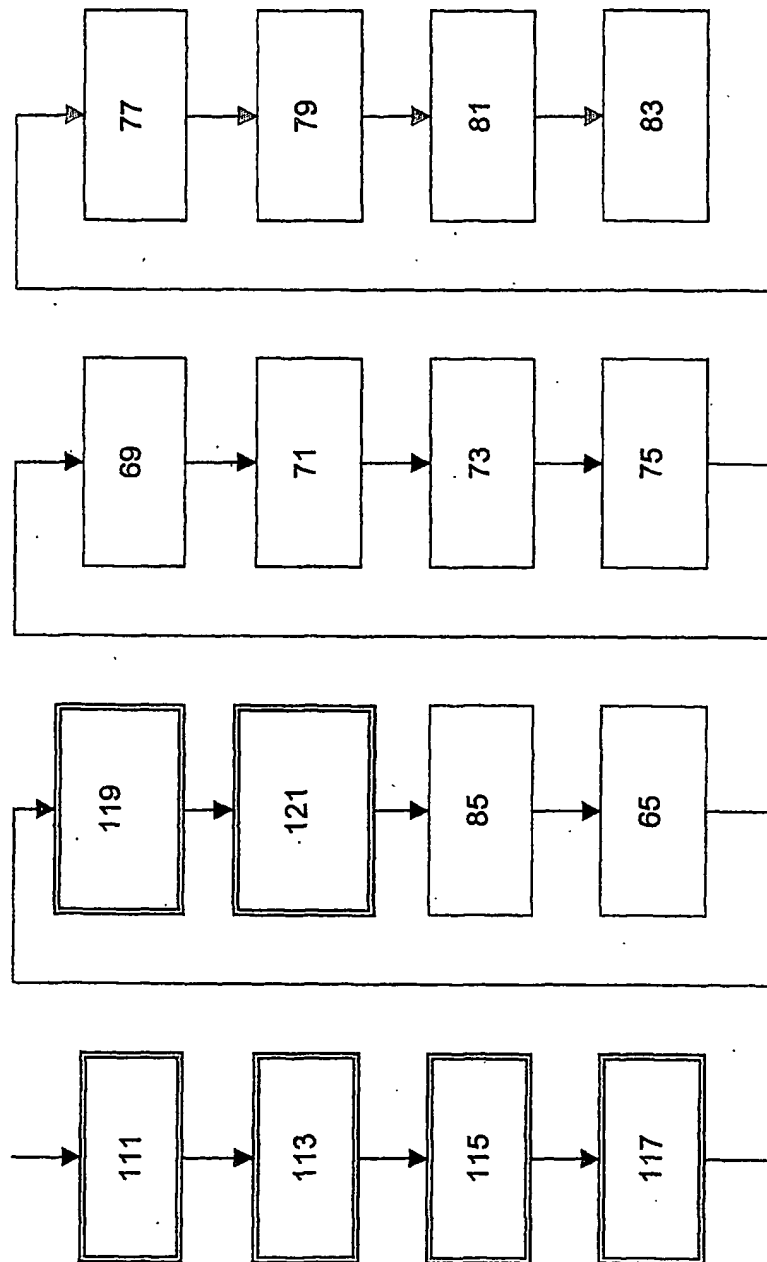


Figure 4B

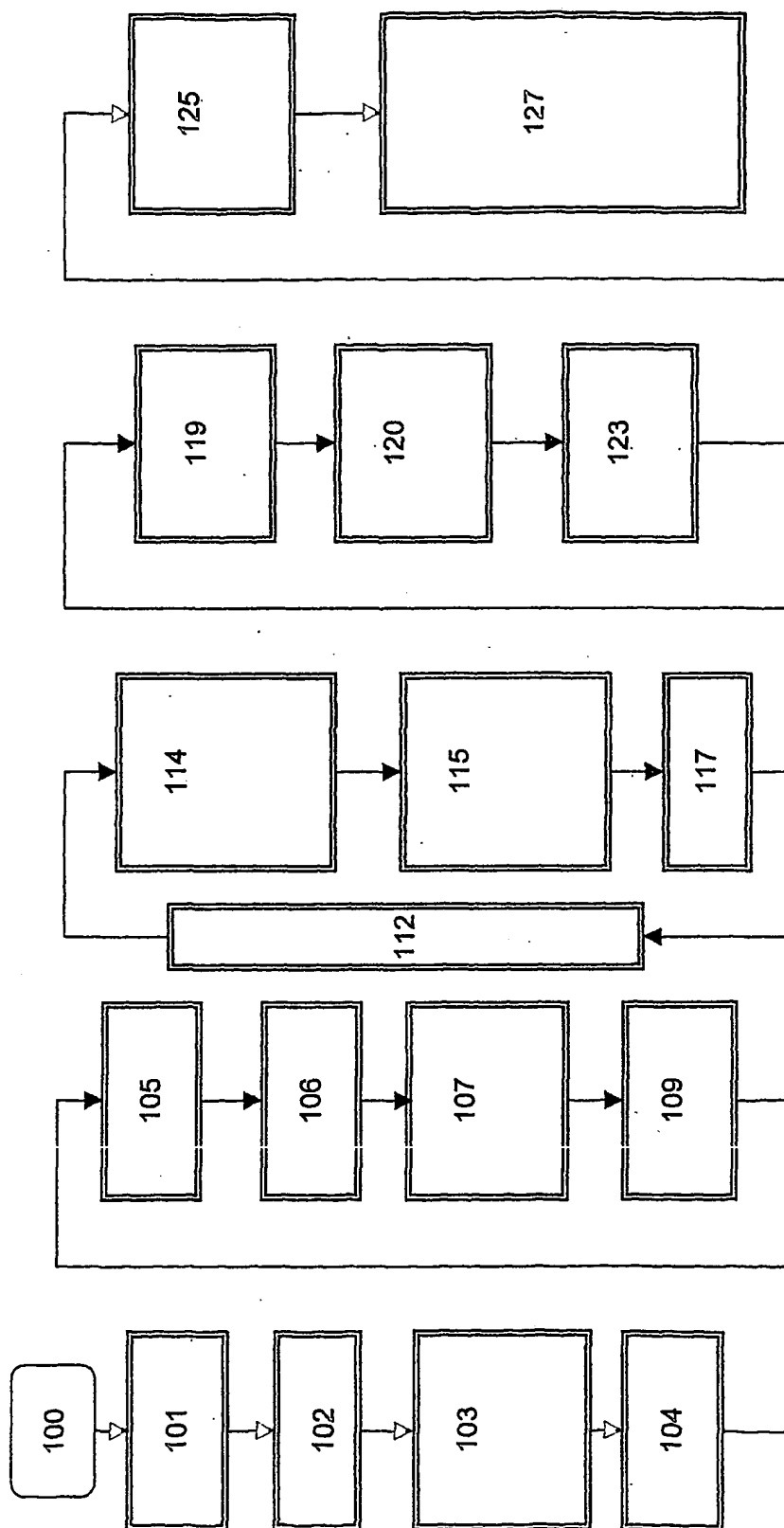


Figure 5

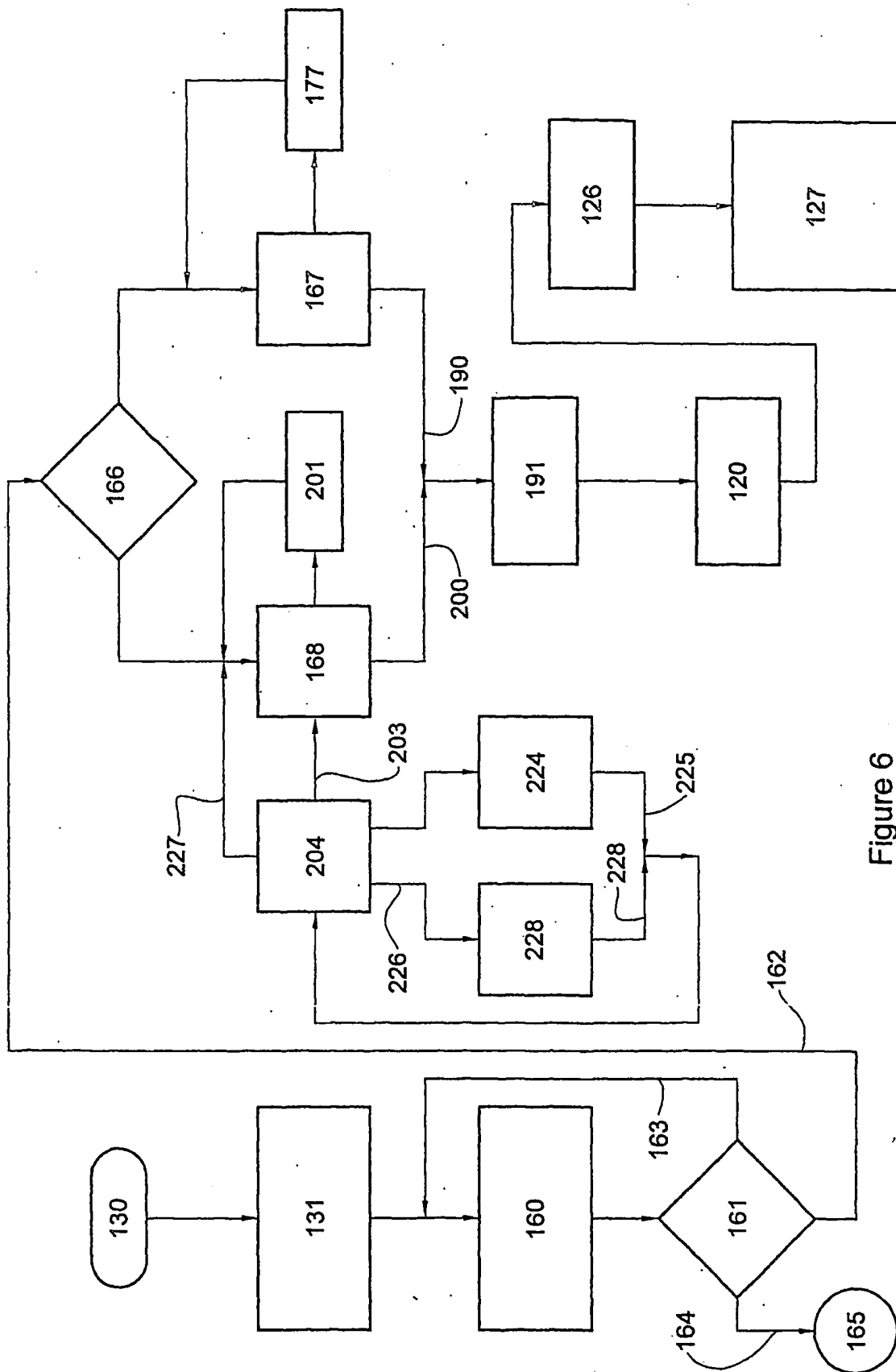


Figure 6

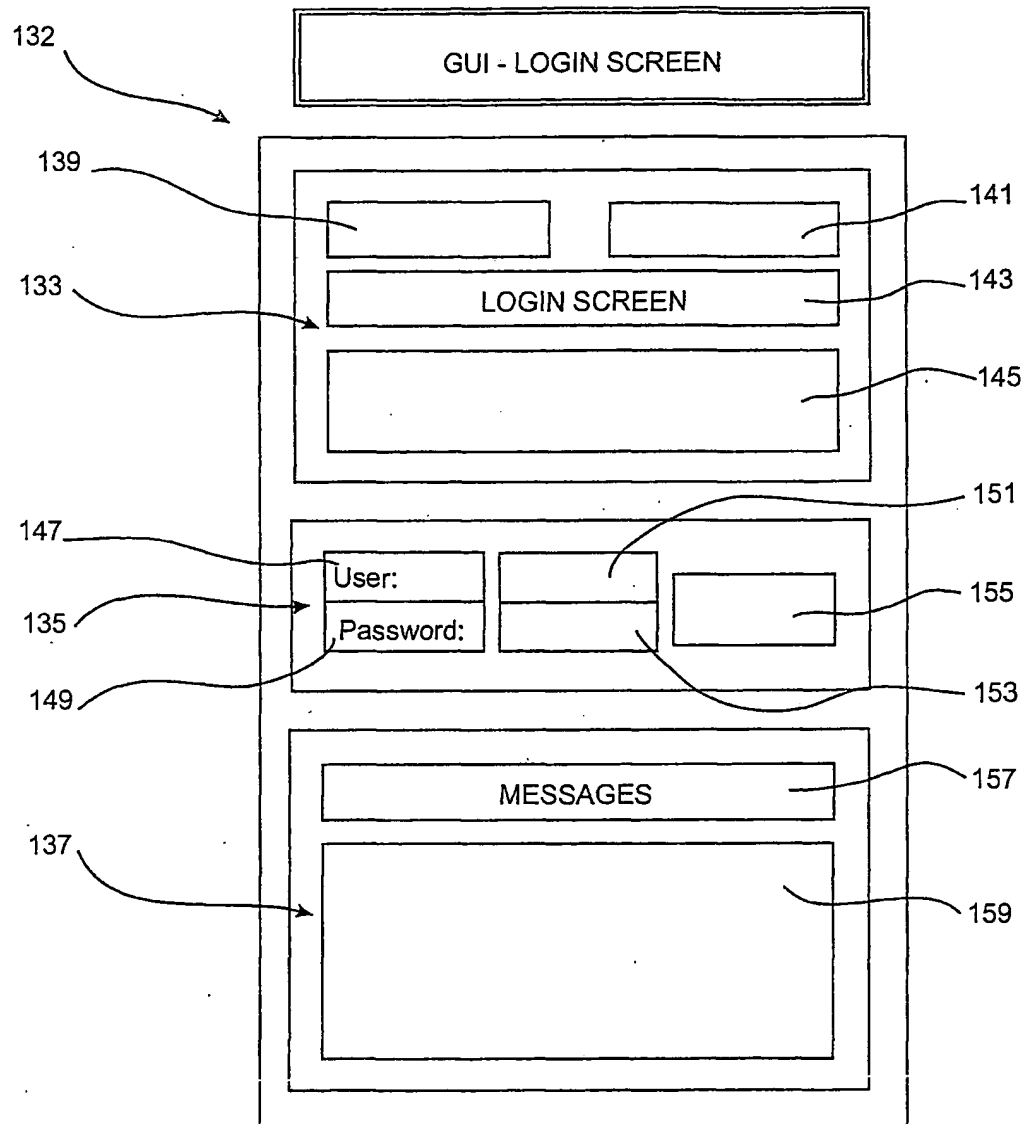


FIG 7 A,

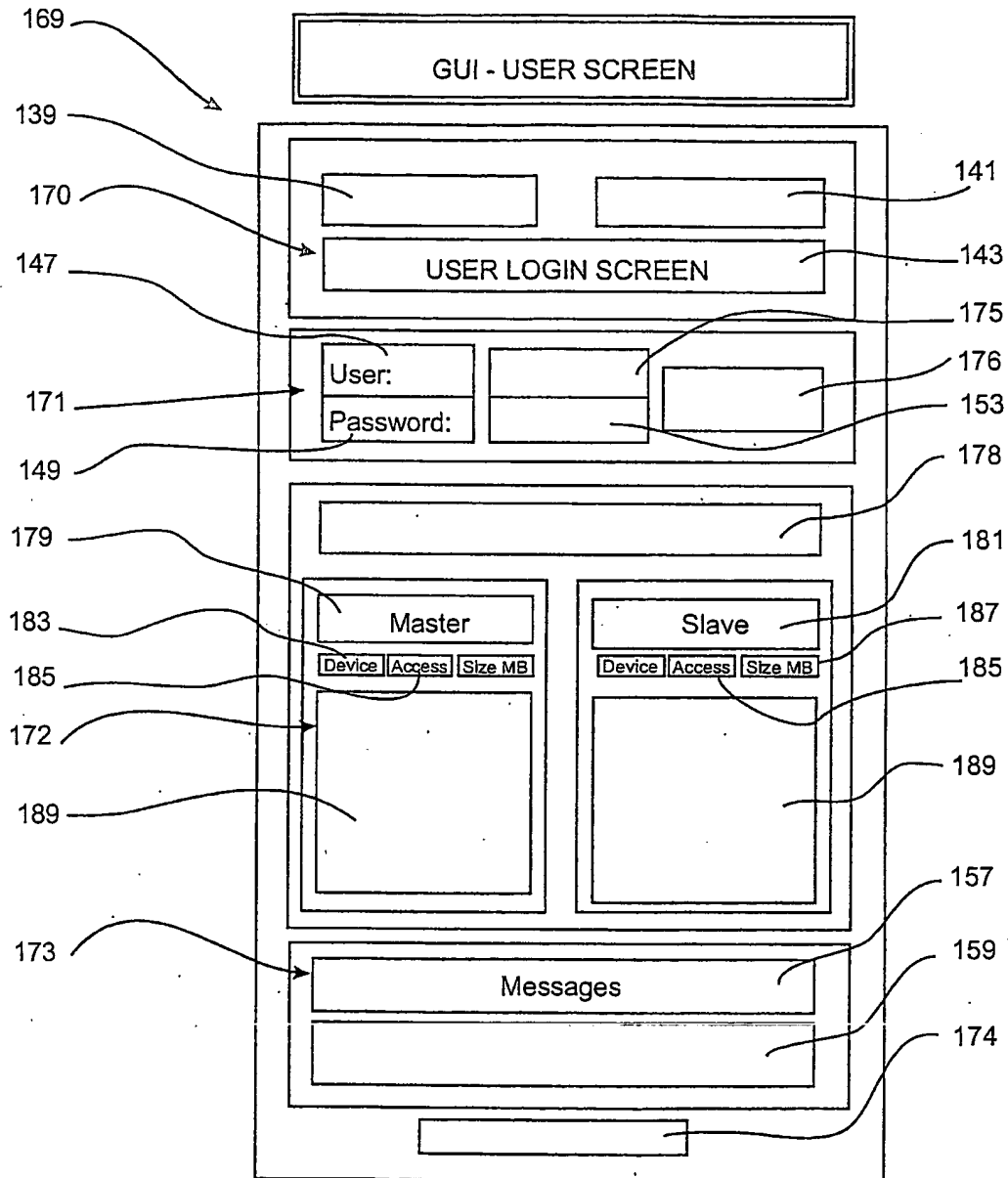
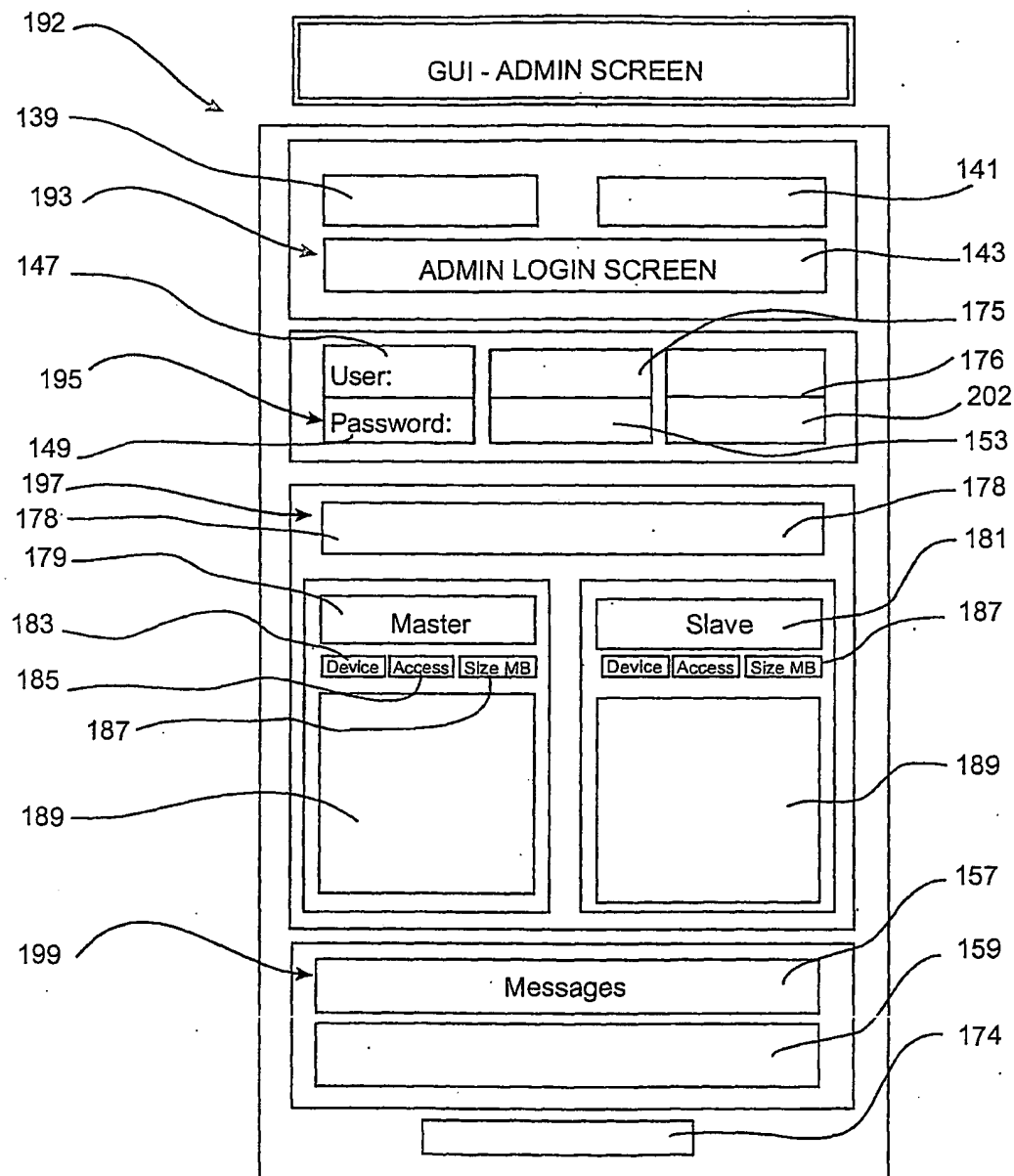
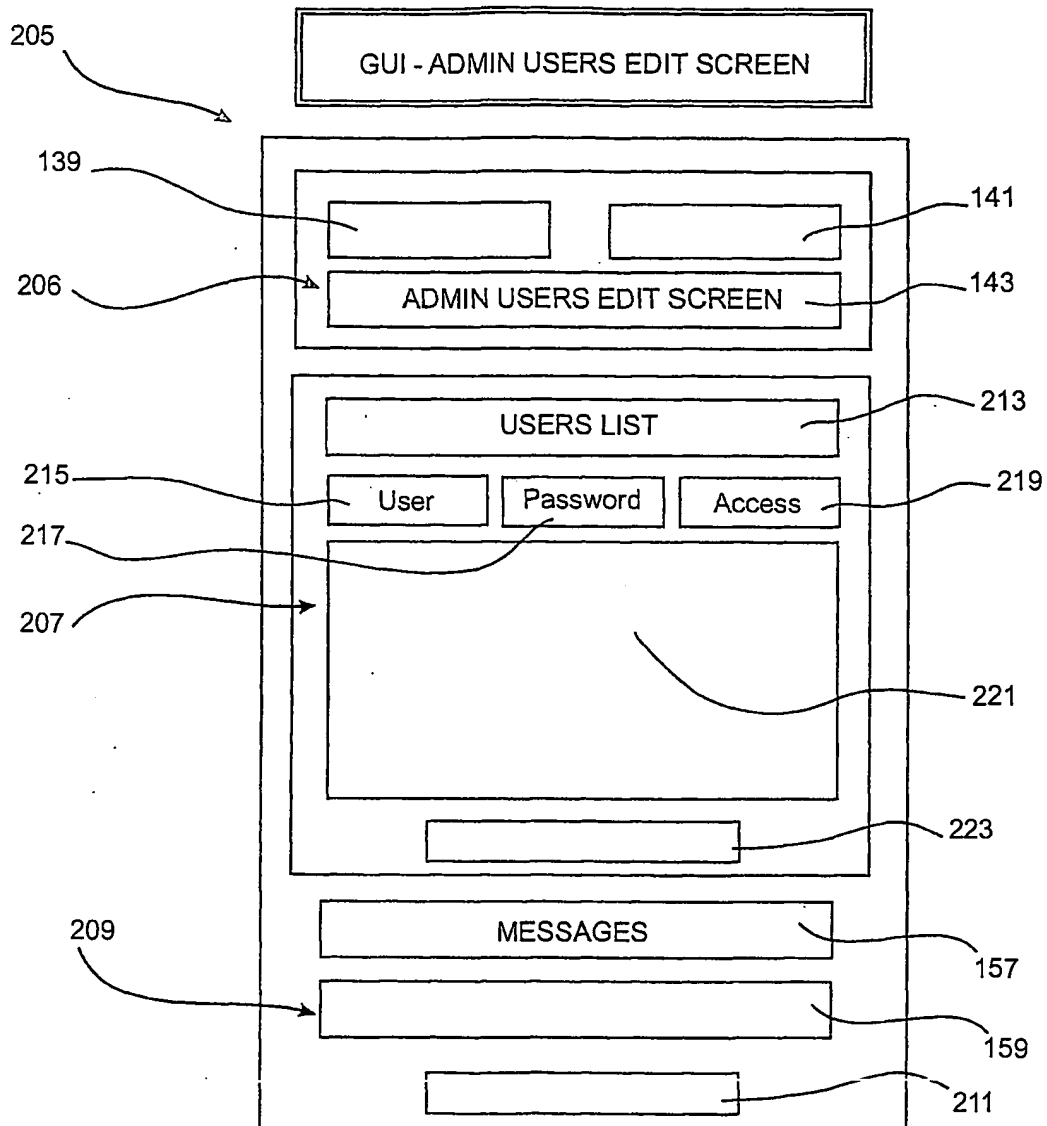


Fig 7B,





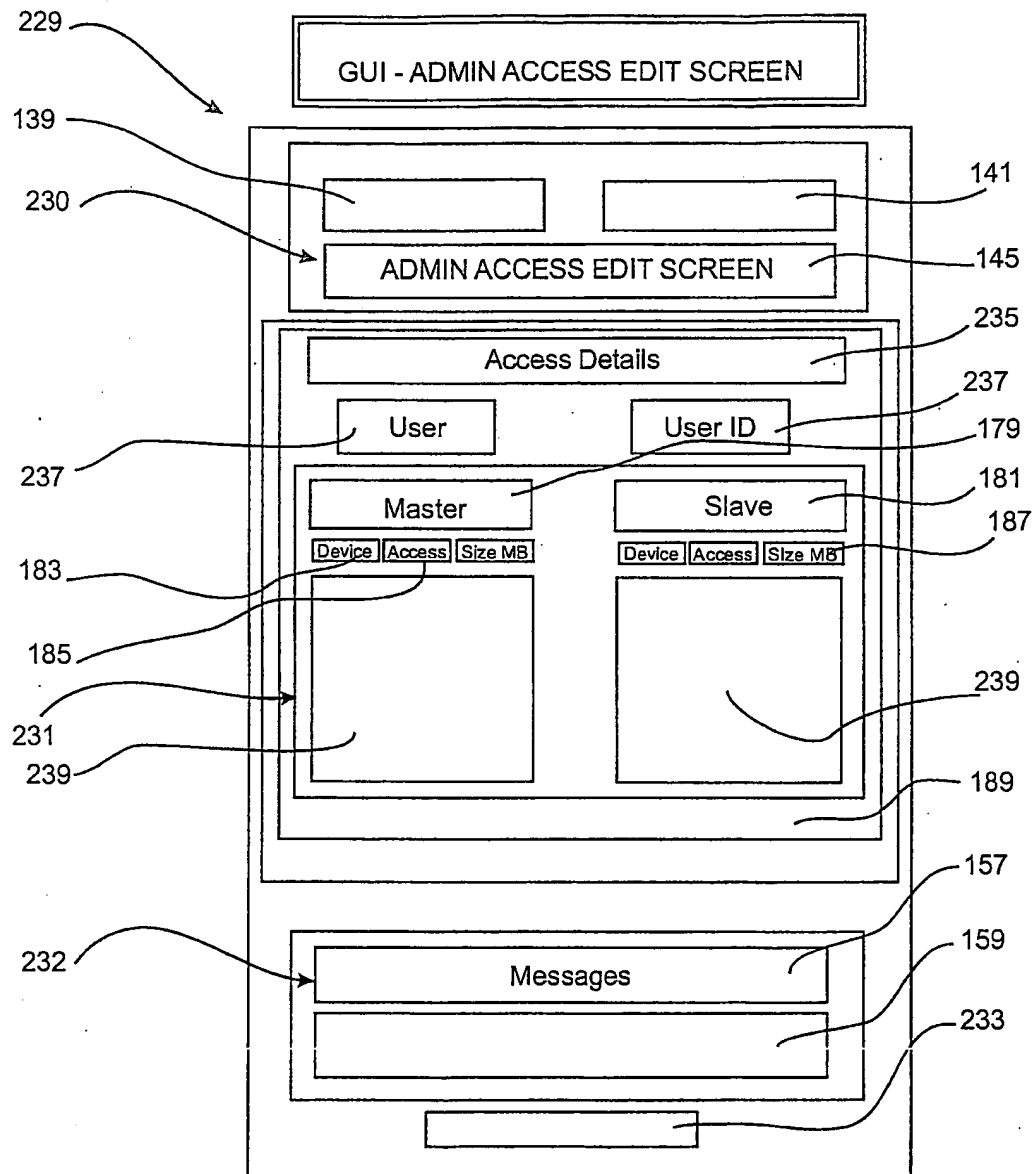


FIG 7 E,

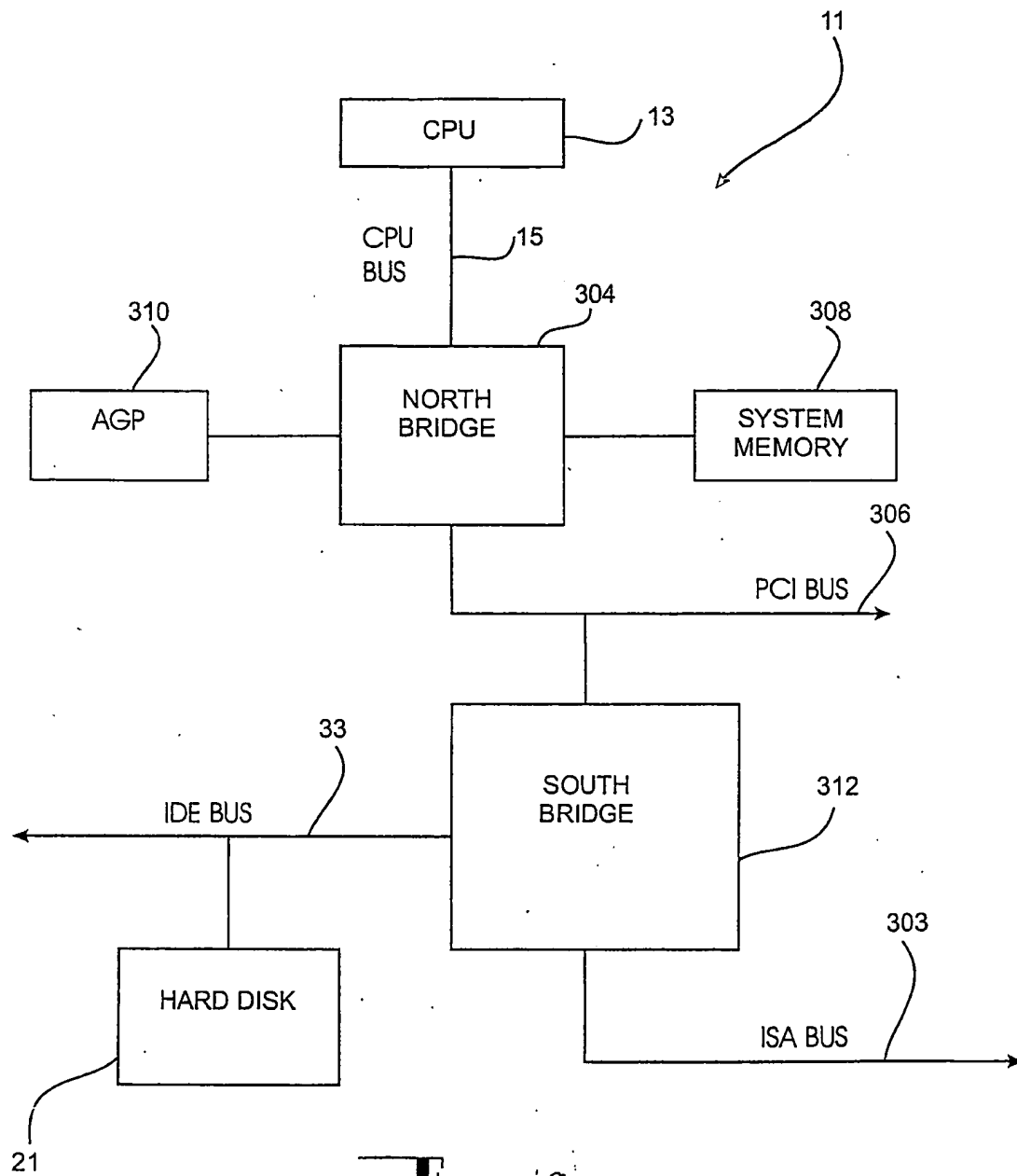
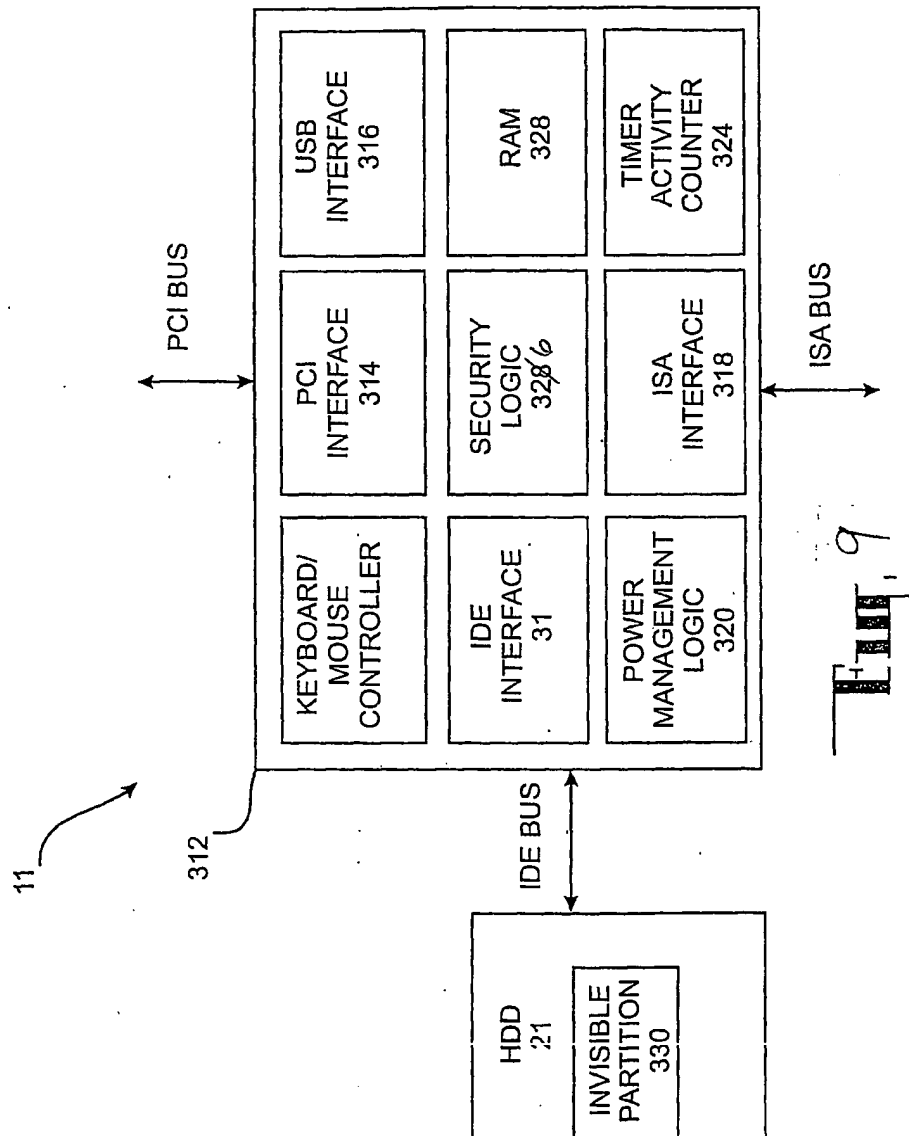
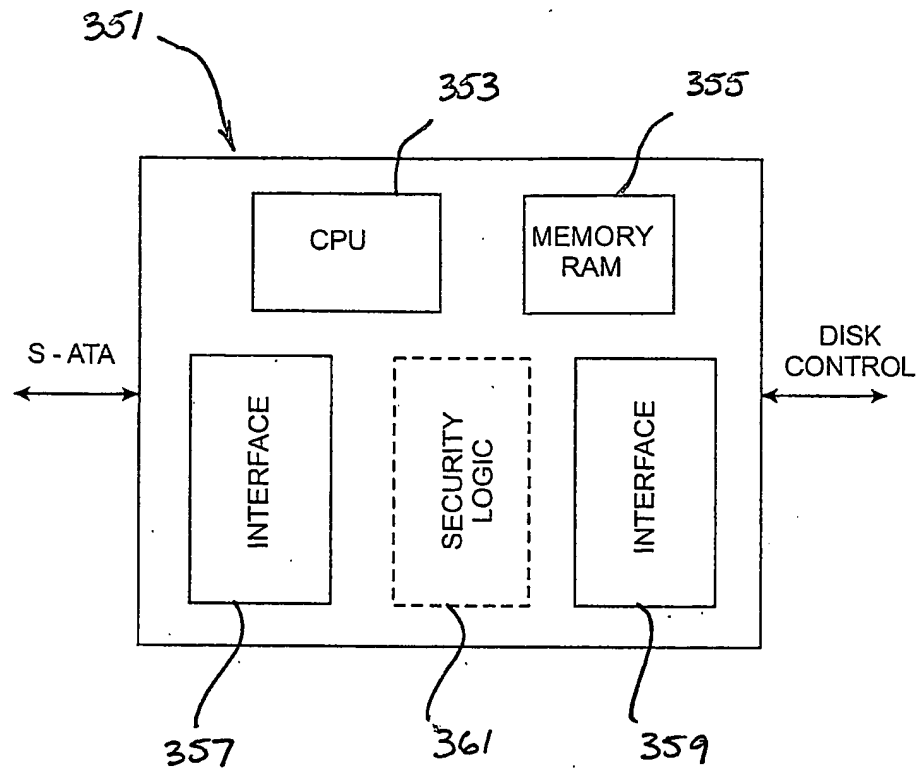


Fig. 8



**Fig. 10**